UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIONRA TECHNOLOGIES LIMITED,

Plaintiff,

v.

FORTINET, INC.,

Defendant.

Case No. 2:22-cv-00322

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Lionra Technologies Limited ("Lionra") files this complaint against Defendant Fortinet Inc., ("Fortinet" or "Defendant") alleging infringement of U.S. Patent Nos. 7,302,708, 7,685,436, 7,921,323, and 8,566,612 ("Patents-in-Suit"). The Accused Products are firewall solutions made, used, offered for sale, sold, imported by Defendant in the United States and supplied by Defendant to their customers and/or integrated into electronic devices sold in the United States.

Plaintiff Lionra and the Patents-in-Suit

1. Plaintiff Lionra is a technology licensing company organized under the laws of Ireland, with its headquarters at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland.

2. Lionra is the owner of U.S. Patent No. 7,302,708 entitled "Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism," which issued November 27, 2007 (the "'708 patent"). A copy of the '708 patent is attached to this complaint as Exhibit 1.

3. Lionra is the owner of U.S. Patent No. 7,685,436, entitled "System and Method for a Secure I/O Interface," which issued March 23, 2010 (the "'436 patent"). A copy of the '436 patent is attached to this complaint as Exhibit 2.

4. Lionra is the owner of U.S. Patent No. 7,921,323, entitled "Reconfigurable Communications Infrastructure for ASIC Networks," which issued April 5, 2011 (the "'323 patent"). A copy of the '323 patent is attached to this complaint as Exhibit 3.

5. Lionra is the owner of U.S. Patent No. 8,566,612, entitled "System and Method for a Secure I/O Interface," which issued October 22, 2013 (the "'612 patent"). A copy of the '612 patent is attached to this complaint as Exhibit 4.

6. On information and belief, Fortinet, Inc. is a Delaware corporation with its principal place of business at 899 Kifer Road, Sunnyvale California 94086. Defendant may be served through its registered agent Corporation Service Company dba CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Defendant is registered to do business in the State of Texas and has been since at least November 24, 2009.

7. With respect to the '708 Patent, the Accused Products include Fortinet's products, including at least FortiWeb Cloud and other Fortinet products with similar functionality.

8. With respect to the '436 Patent, the Accused Products include Fortinet's products, including at least the FortiGate-7060 and other Fortinet products with similar functionality.

9. With respect to the '323 Patent, the Accused Products include Fortinet's products, including at least the FortiGate-7121F and other Fortinet products with similar functionality.

10. With respect to the '612 Patent, the Accused Products include Fortinet's products, including at least the FortiGate-7060 and other Fortinet products with similar functionality.

Jurisdiction and Venue

11. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over Defendant in this action because, among other reasons, Defendant has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with the forum state of Texas. Defendant maintains a place of business within the State, including at 6111 W. Plano Parkway, Plano, Texas 75093. Defendant directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, making, using, importing, offering for sale, and/or selling products and/or services that infringe the patents-in-suit. Thus, Defendant purposefully availed itself of the benefits of doing business in the State of Texas and the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice. Defendant is registered to do business in the State of Texas, and has appointed as their registered agent, Corporation Service Company dba CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701, for service of process.

13. Venue is proper in this district under 28 U.S.C. §1400(b) and 28 U.S.C. §§ 1391(c). Defendant has a regular and established place of business in this district at least as set forth above.

Count 1 – Claim for infringement of the ’708 patent.

14. Lionra incorporates by reference each of the allegations in paragraphs 1–13 above and further alleges as follows:

15. On November 27, 2007, the United States Patent and Trademark Office issued U.S. Patent No. 7,302,708 entitled "Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism." Ex. 1.

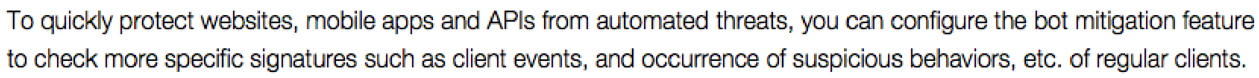
16. Lionra is the owner of the '708 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

17. Each claim of the '708 patent is valid, enforceable, and patent-eligible.

18. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the '708 patent, and Lionra is entitled to damages for Defendant's past infringement.

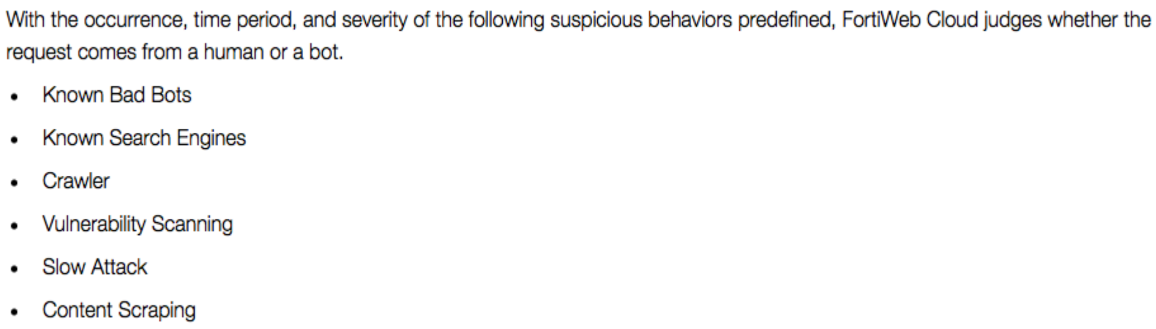
19. Defendant has directly infringed (literally and equivalently) and induced others to infringe the '708 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the '708 patent and by inducing others to infringe the claims of the '708 patent without a license or permission from Lionra. These products include without limitation, Defendant's products, including at least the FortiWeb Cloud, which infringes at least claim 1 of the '708 patent.

20. On information and belief, whether or not the preamble is deemed limiting, the FortiWeb Cloud performs a method for secure access to a computer system.



To quickly protect websites, mobile apps and APIs from automated threats, you can configure the bot mitigation feature to check more specific signatures such as client events, and occurrence of suspicious behaviors, etc. of regular clients.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/477089/bot-mitigation

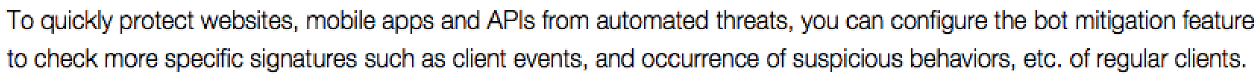


With the occurrence, time period, and severity of the following suspicious behaviors predefined, FortiWeb Cloud judges whether the request comes from a human or a bot.

- Known Bad Bots
- Known Search Engines
- Crawler
- Vulnerability Scanning
- Slow Attack
- Content Scraping

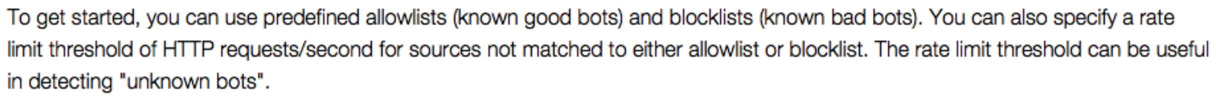
See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/912809/threshold-based-detection

21. On information and belief, the FortiWeb Cloud receives in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function.



To quickly protect websites, mobile apps and APIs from automated threats, you can configure the bot mitigation feature to check more specific signatures such as client events, and occurrence of suspicious behaviors, etc. of regular clients.

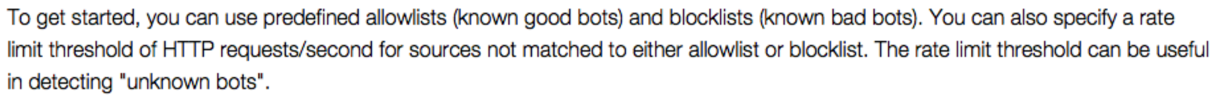
See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/477089/bot-mitigation



To get started, you can use predefined allowlists (known good bots) and blocklists (known bad bots). You can also specify a rate limit threshold of HTTP requests/second for sources not matched to either allowlist or blocklist. The rate limit threshold can be useful in detecting "unknown bots".

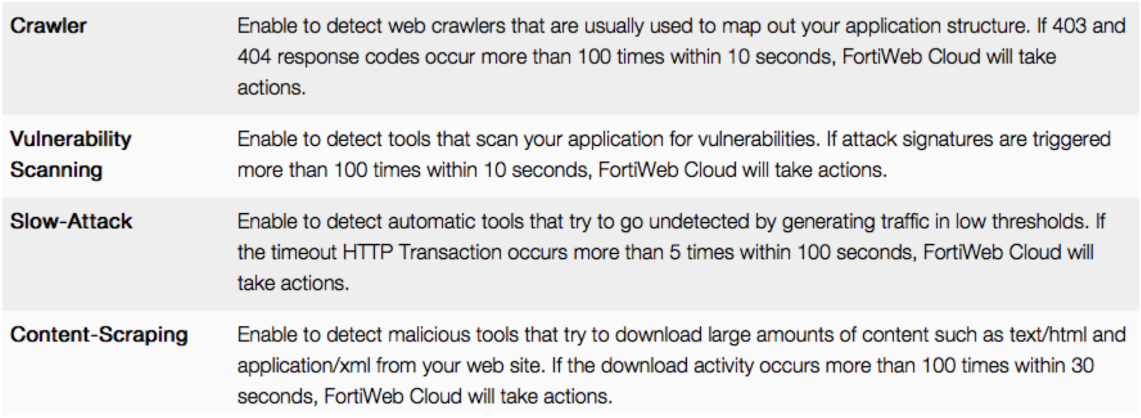
See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection

22. On information and belief, FortiWeb Cloud determines if said access request completes a prohibited temporal access pattern for said entity.

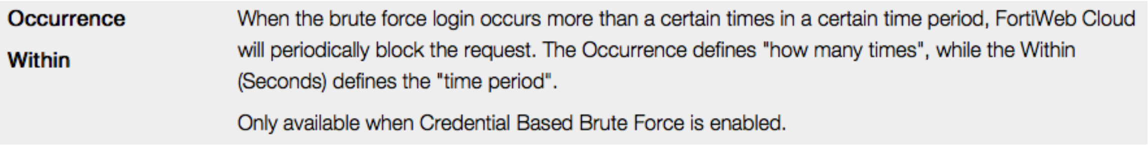


To get started, you can use predefined allowlists (known good bots) and blocklists (known bad bots). You can also specify a rate limit threshold of HTTP requests/second for sources not matched to either allowlist or blocklist. The rate limit threshold can be useful in detecting "unknown bots".

See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection

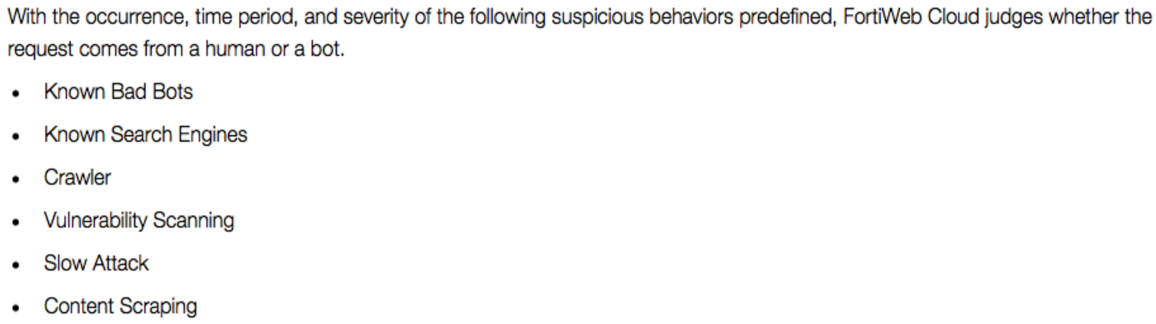


Crawler	Enable to detect web crawlers that are usually used to map out your application structure. If 403 and 404 response codes occur more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Vulnerability Scanning	Enable to detect tools that scan your application for vulnerabilities. If attack signatures are triggered more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Slow-Attack	Enable to detect automatic tools that try to go undetected by generating traffic in low thresholds. If the timeout HTTP Transaction occurs more than 5 times within 100 seconds, FortiWeb Cloud will take actions.
Content-Scraping	Enable to detect malicious tools that try to download large amounts of content such as text/html and application/xml from your web site. If the download activity occurs more than 100 times within 30 seconds, FortiWeb Cloud will take actions.



Occurrence **Within**	When the brute force login occurs more than a certain times in a certain time period, FortiWeb Cloud will periodically block the request. The Occurrence defines "how many times", while the Within (Seconds) defines the "time period". Only available when Credential Based Brute Force is enabled.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/912809/threshold-based-detection

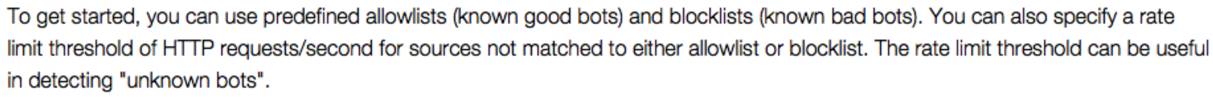


With the occurrence, time period, and severity of the following suspicious behaviors predefined, FortiWeb Cloud judges whether the request comes from a human or a bot.

- Known Bad Bots
- Known Search Engines
- Crawler
- Vulnerability Scanning
- Slow Attack
- Content Scraping

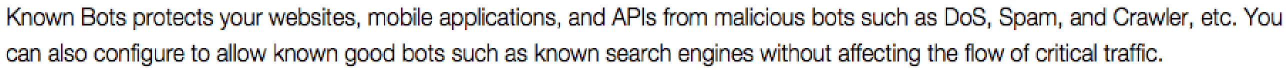
See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/912809/threshold-based-detection

23. On information and belief, FortiWeb Cloud compares a minimum access level established for said first base node to said predetermined access level.



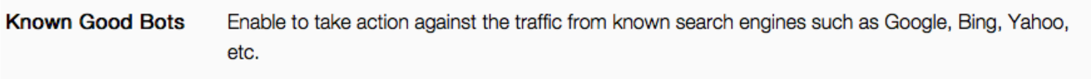
To get started, you can use predefined allowlists (known good bots) and blocklists (known bad bots). You can also specify a rate limit threshold of HTTP requests/second for sources not matched to either allowlist or blocklist. The rate limit threshold can be useful in detecting "unknown bots".

See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection



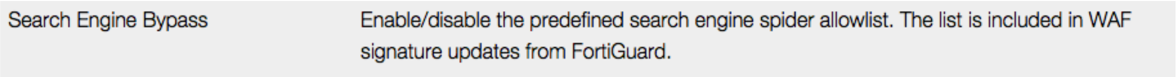
Known Bots protects your websites, mobile applications, and APIs from malicious bots such as DoS, Spam, and Crawler, etc. You can also configure to allow known good bots such as known search engines without affecting the flow of critical traffic.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/767135/known-bots



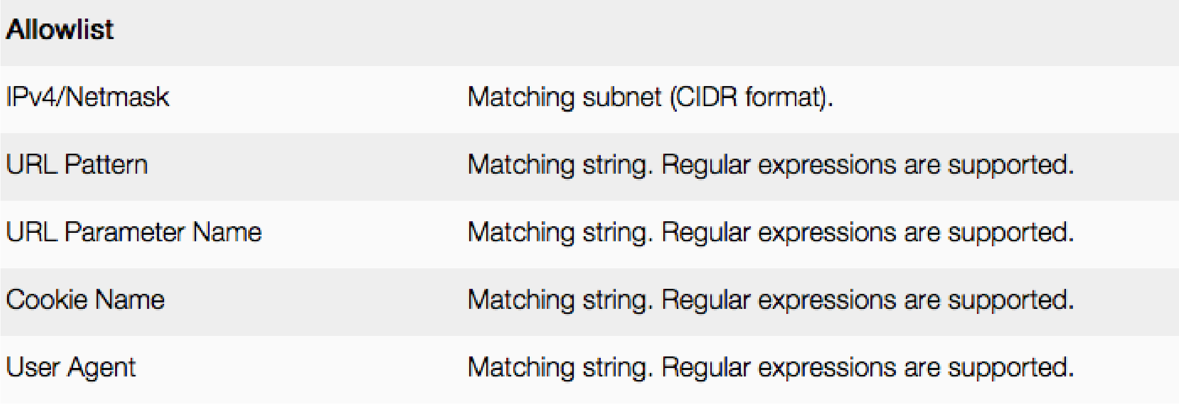
Known Good Bots	Enable to take action against the traffic from known search engines such as Google, Bing, Yahoo, etc.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/767135/known-bots



Search Engine Bypass	Enable/disable the predefined search engine spider allowlist. The list is included in WAF signature updates from FortiGuard.

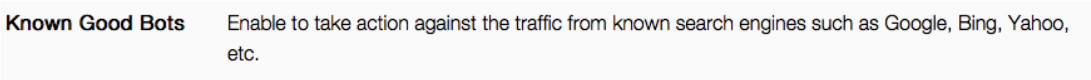
See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection



Allowlist	
IPv4/Netmask	Matching subnet (CIDR format).
URL Pattern	Matching string. Regular expressions are supported.
URL Parameter Name	Matching string. Regular expressions are supported.
Cookie Name	Matching string. Regular expressions are supported.
User Agent	Matching string. Regular expressions are supported.

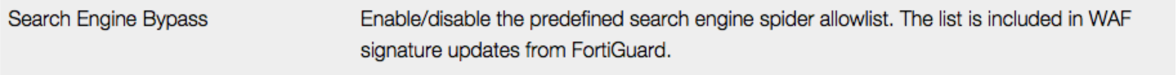
See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection

24. On information and belief, FortiWeb Cloud grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.



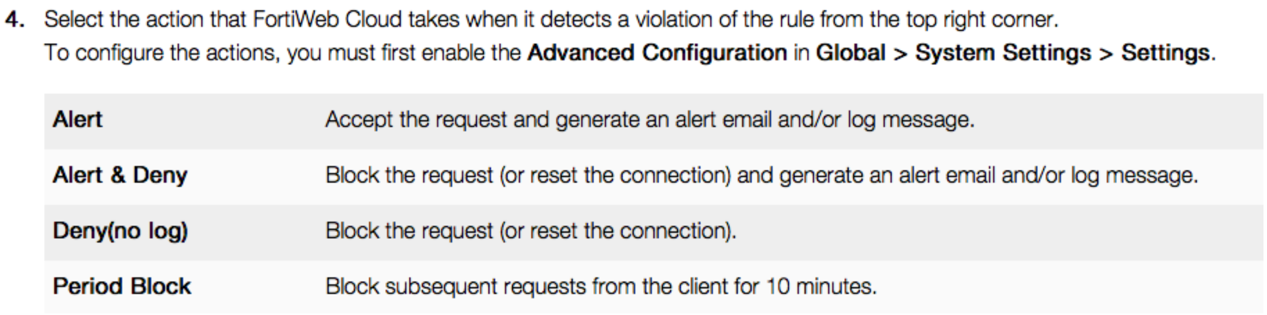
Known Good Bots	Enable to take action against the traffic from known search engines such as Google, Bing, Yahoo, etc.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/767135/known-bots



Search Engine Bypass	Enable/disable the predefined search engine spider allowlist. The list is included in WAF signature updates from FortiGuard.

See https://docs.fortinet.com/document/fortiadc/7.0.2/handbook/43621/configuring-a-bot-detection-policy#bot_detection

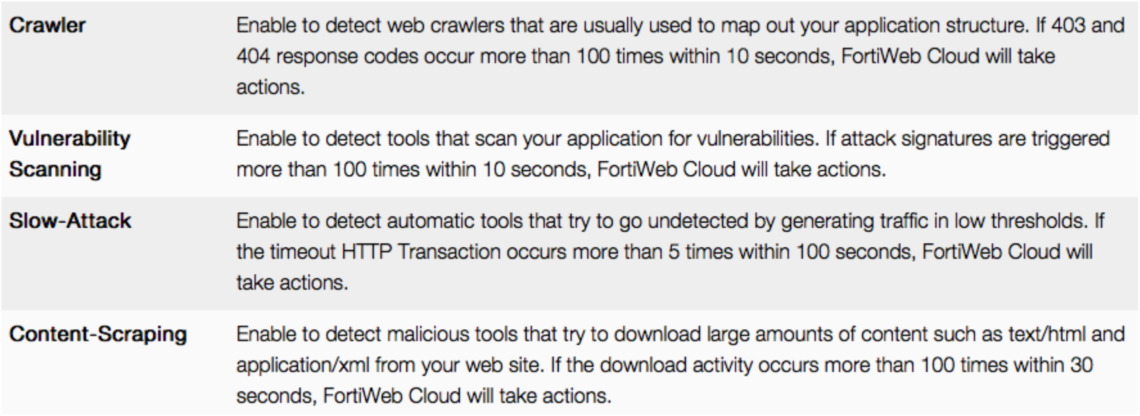


4. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
To configure the actions, you must first enable the **Advanced Configuration** in **Global** > **System Settings** > **Settings**.

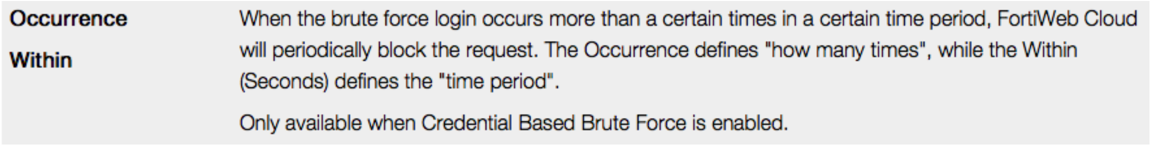
Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block subsequent requests from the client for 10 minutes.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/767135/known-bots

25. On information and belief, FortiWeb Cloud denying said request if said access request completes a prohibited temporal access pattern for said entity.

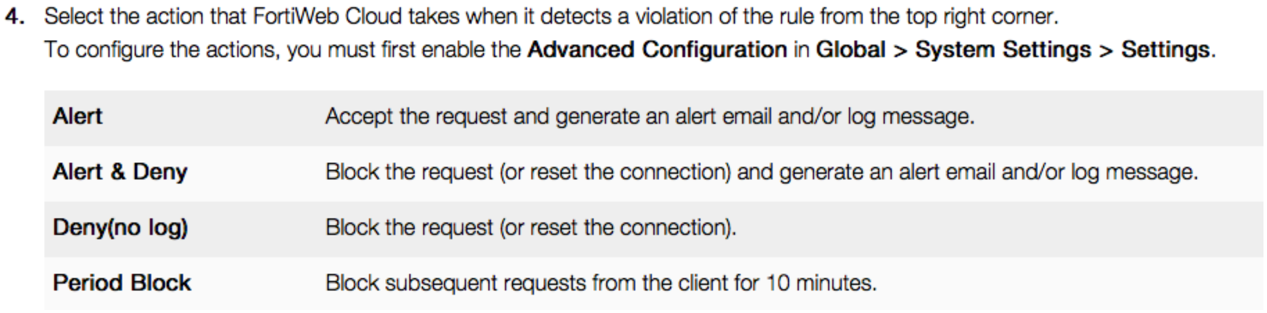


Crawler	Enable to detect web crawlers that are usually used to map out your application structure. If 403 and 404 response codes occur more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Vulnerability Scanning	Enable to detect tools that scan your application for vulnerabilities. If attack signatures are triggered more than 100 times within 10 seconds, FortiWeb Cloud will take actions.
Slow-Attack	Enable to detect automatic tools that try to go undetected by generating traffic in low thresholds. If the timeout HTTP Transaction occurs more than 5 times within 100 seconds, FortiWeb Cloud will take actions.
Content-Scraping	Enable to detect malicious tools that try to download large amounts of content such as text/html and application/xml from your web site. If the download activity occurs more than 100 times within 30 seconds, FortiWeb Cloud will take actions.



Occurrence **Within**	When the brute force login occurs more than a certain times in a certain time period, FortiWeb Cloud will periodically block the request. The Occurrence defines "how many times", while the Within (Seconds) defines the "time period". Only available when Credential Based Brute Force is enabled.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/912809/threshold-based-detection



4. Select the action that FortiWeb Cloud takes when it detects a violation of the rule from the top right corner.
To configure the actions, you must first enable the **Advanced Configuration** in **Global** > **System Settings** > **Settings**.

Alert	Accept the request and generate an alert email and/or log message.
Alert & Deny	Block the request (or reset the connection) and generate an alert email and/or log message.
Deny(no log)	Block the request (or reset the connection).
Period Block	Block subsequent requests from the client for 10 minutes.

See https://docs.fortinet.com/document/fortiweb-cloud/latest/user-guide/767135/known-bots

Count 2 – Claim for infringement of the ’436 patent.

26. Lionra incorporates by reference each of the allegations in paragraphs 1–25 above and further alleges as follows:

27. On March 23, 2010, the United States Patent and Trademark Office issued U.S. Patent No. 7,685,436, entitled “System and Method for a Secure I/O Interface.” Ex. 2.

28. Lionra is the owner of the ’436 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

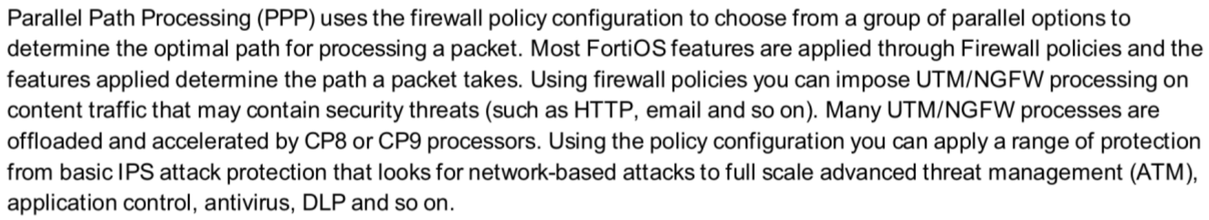
29. Each claim of the ’436 patent is valid, enforceable, and patent-eligible.

30. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’436 patent, and Lionra is entitled to damages for Defendant’s past infringement.

31. Defendant have directly infringed (literally and equivalently) and induced others to infringe the ’436 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’436 patent and by inducing others to infringe the claims of the ’436 patent without a license or permission from Lionra. These products include without limitation Defendant’s FortiGate-7060E, which infringes at least claim 1 of the ’436 patent.

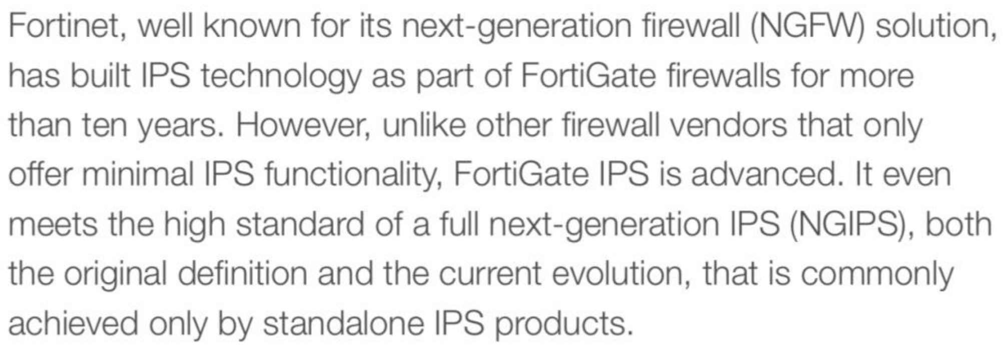
32. Defendant also has indirectly infringed at least one claim of the ’436 patent contributorily under 35 U.S.C. § 271(c) by offering to sell and selling the Accused Products, knowing the same to be especially made or especially adapted for use in an infringement of the ’436 patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. They do not have any substantial non-infringing uses.

33. On information and belief, whether or not the preamble is limiting, FortiGate-7060E is a security processor for processing incoming packets and outgoing packets.



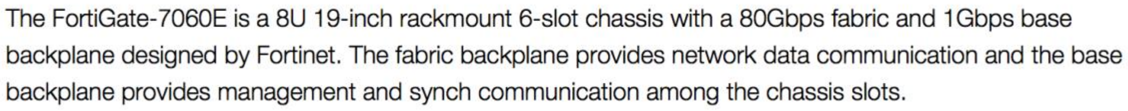
Parallel Path Processing (PPP) uses the firewall policy configuration to choose from a group of parallel options to determine the optimal path for processing a packet. Most FortiOS features are applied through Firewall policies and the features applied determine the path a packet takes. Using firewall policies you can impose UTM/NGFW processing on content traffic that may contain security threats (such as HTTP, email and so on). Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors. Using the policy configuration you can apply a range of protection from basic IPS attack protection that looks for network-based attacks to full scale advanced threat management (ATM), application control, antivirus, DLP and so on.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 6 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



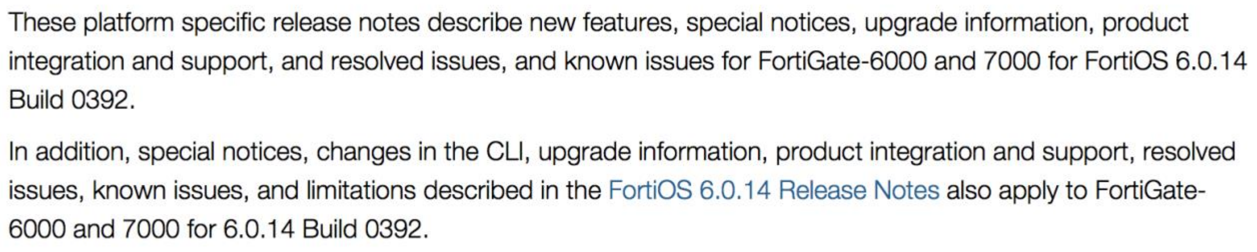
Fortinet, well known for its next-generation firewall (NGFW) solution, has built IPS technology as part of FortiGate firewalls for more than ten years. However, unlike other firewall vendors that only offer minimal IPS functionality, FortiGate IPS is advanced. It even meets the high standard of a full next-generation IPS (NGIPS), both the original definition and the current evolution, that is commonly achieved only by standalone IPS products.

See Powerful and Innovative Intrusion Prevention Systems FortiGate IPS at p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-FortiGateIPS.pdf



The FortiGate-7060E is a 8U 19-inch rackmount 6-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

See https://docs.fortinet.com/document/fortigate/6.0.14/fortigate-7000-documents/64586/fortigate-7060e

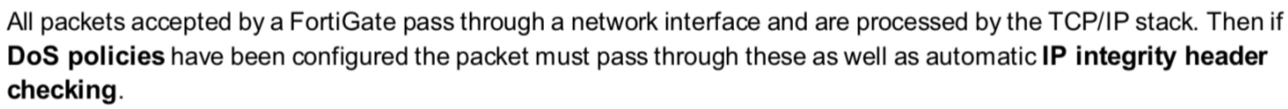


These platform specific release notes describe new features, special notices, upgrade information, product integration and support, and resolved issues, and known issues for FortiGate-6000 and 7000 for FortiOS 6.0.14 Build 0392.

In addition, special notices, changes in the CLI, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.0.14 Release Notes also apply to FortiGate-6000 and 7000 for 6.0.14 Build 0392.

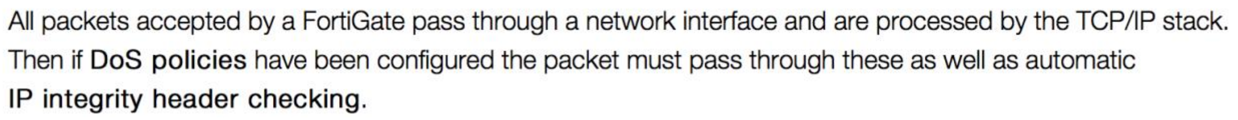
See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000-release-notes/575159/fortigate-6000-and-fortigate-7000-6-0-14-release-notes

34. On information and belief, the FortiGate-7060E includes a switching system to send the outgoing packets and receive the incoming packets.



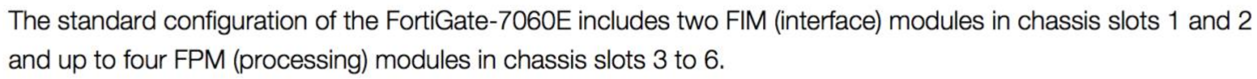
All packets accepted by a FortiGate pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking**.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 9 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



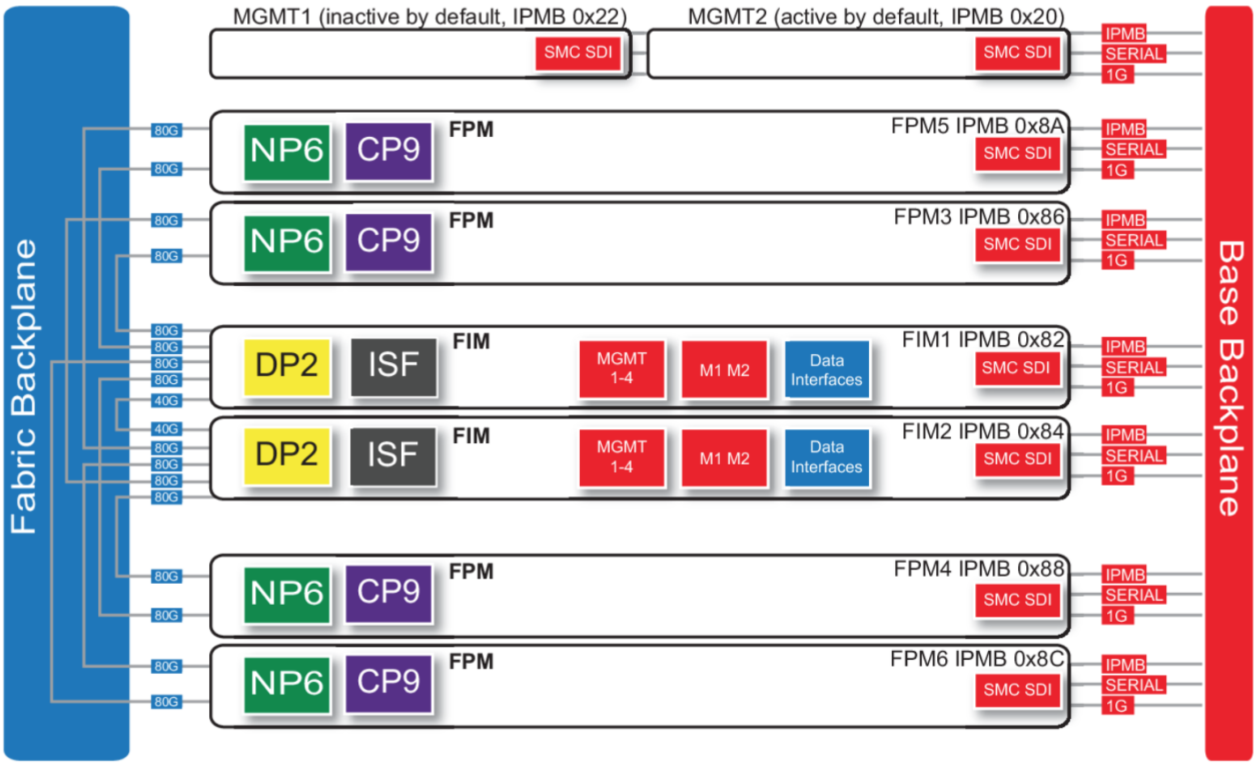
All packets accepted by a FortiGate pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking**.

See https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

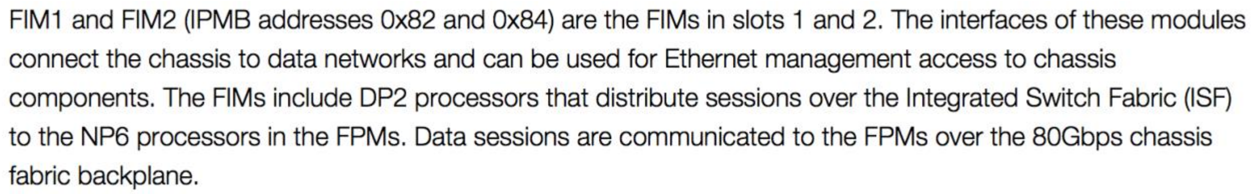


The standard configuration of the FortiGate-7060E includes two FIM (interface) modules in chassis slots 1 and 2 and up to four FPM (processing) modules in chassis slots 3 to 6.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e



See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e

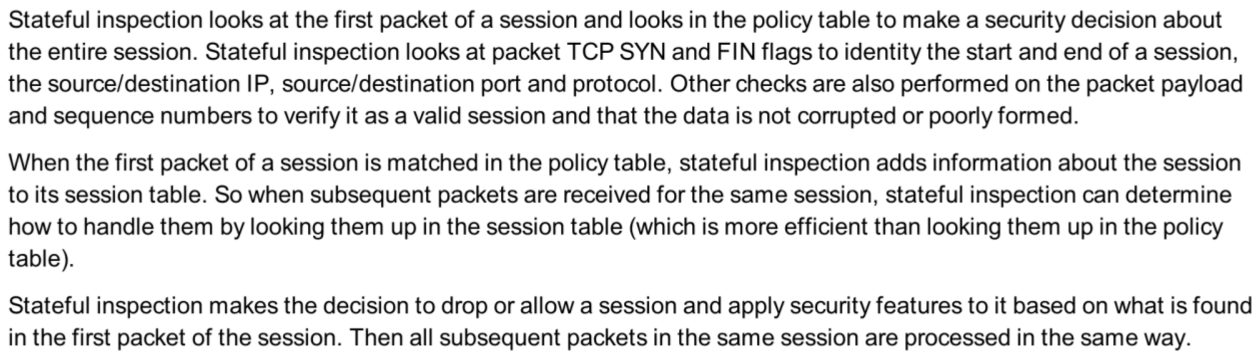


FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e

35. On information and belief, the FortiGate-7060E includes a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one

of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core.

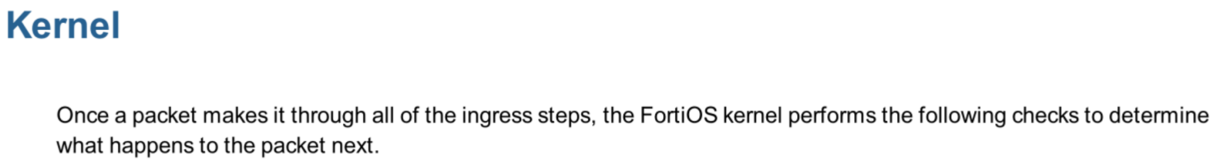


Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed.

When the first packet of a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).

Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way.

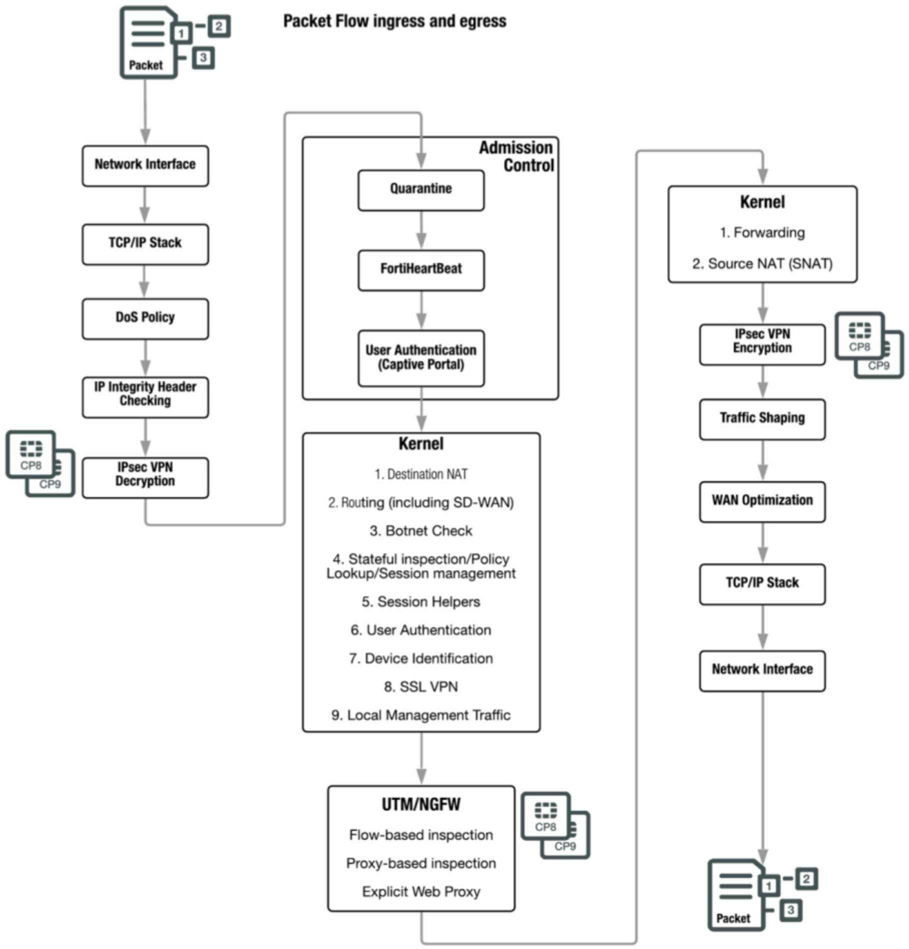
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 10 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



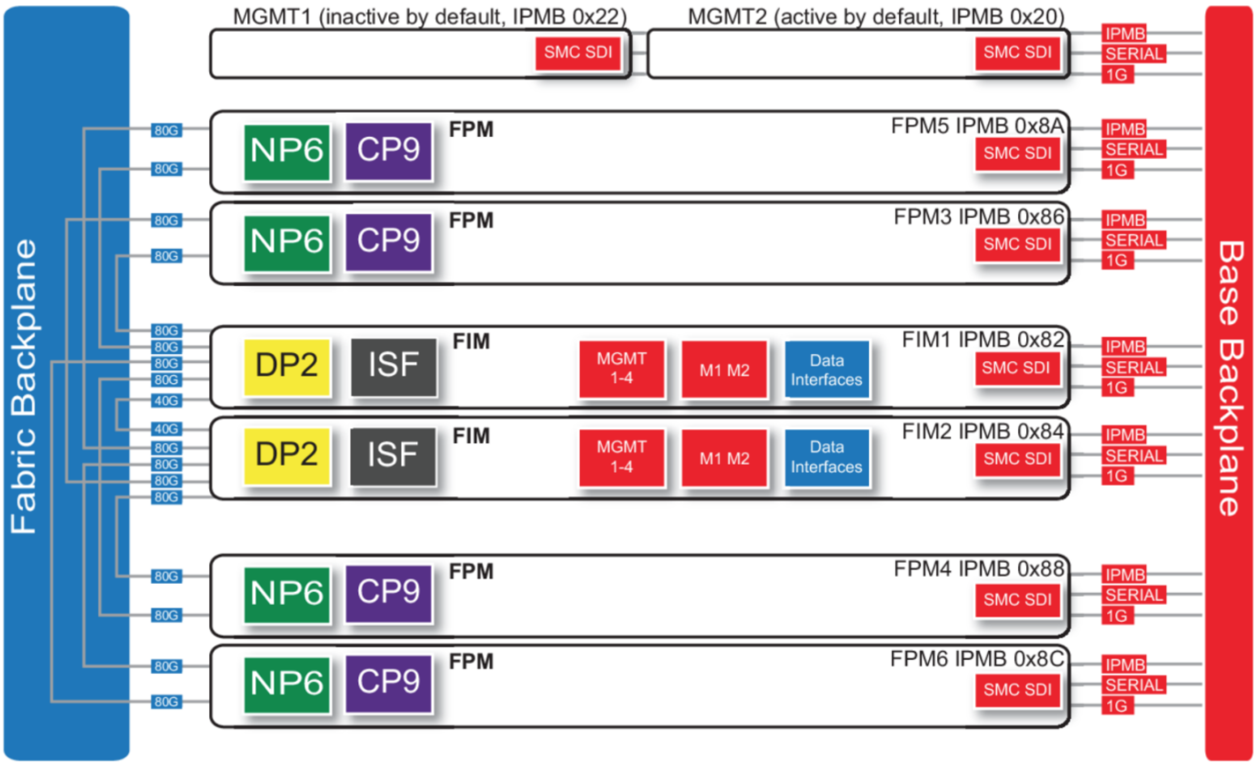
Kernel

Once a packet makes it through all of the ingress steps, the FortiOS kernel performs the following checks to determine what happens to the packet next.

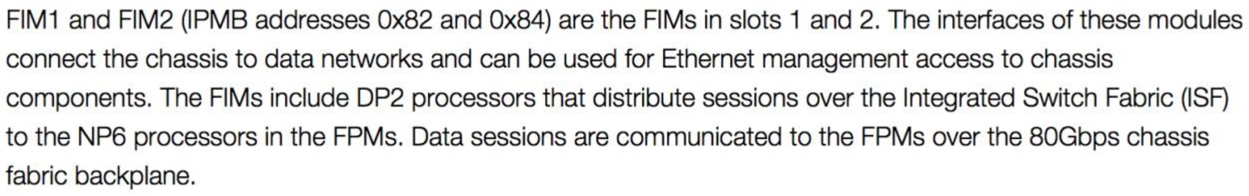
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 9 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



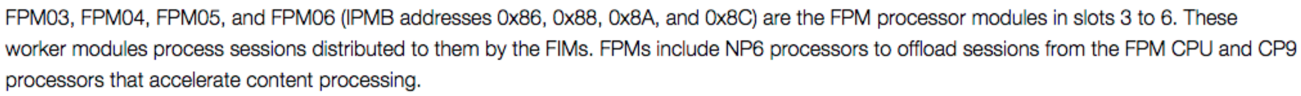
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 8 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



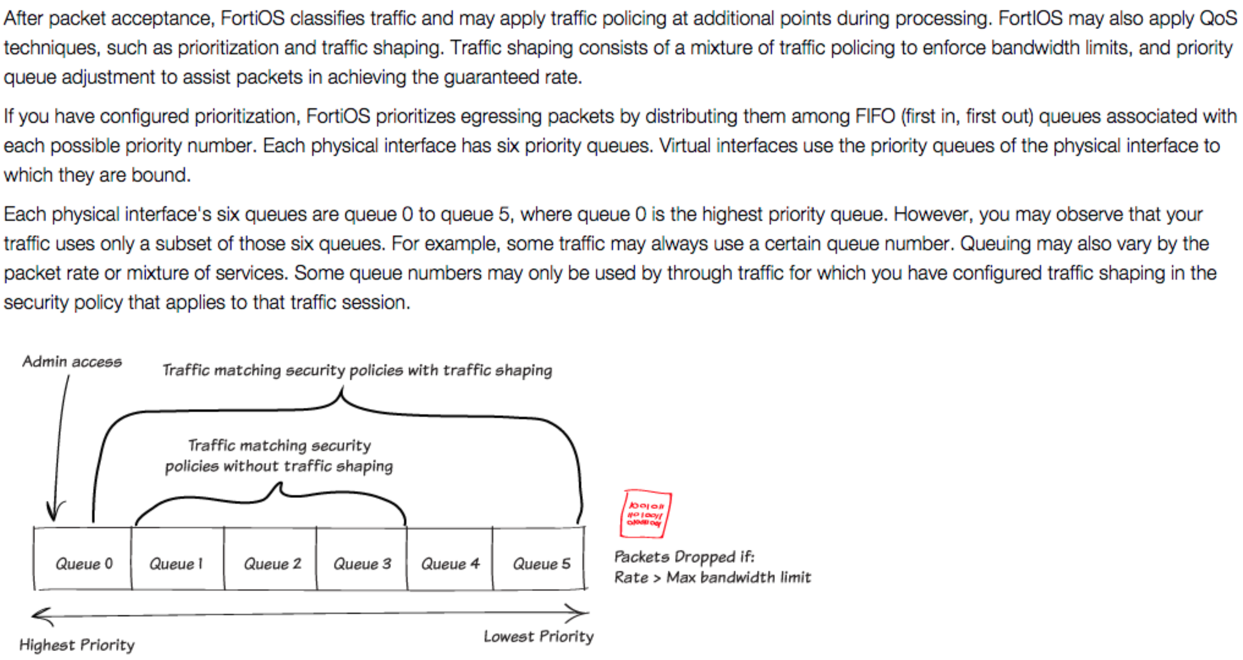
See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e


FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e


FPM03, FPM04, FPM05, and FPM06 (IPMB addresses 0x86, 0x88, 0x8A, and 0x8C) are the FPM processor modules in slots 3 to 6. These worker modules process sessions distributed to them by the FIMs. FPMs include NP6 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e



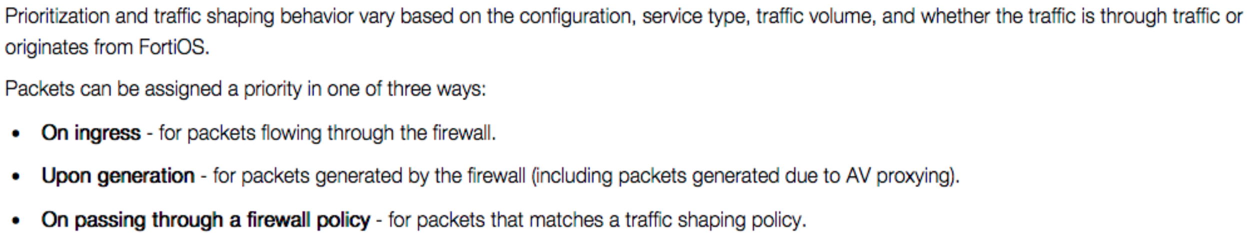
After packet acceptance, FortiOS classifies traffic and may apply traffic policing at additional points during processing. FortIOS may also apply QoS techniques, such as prioritization and traffic shaping. Traffic shaping consists of a mixture of traffic policing to enforce bandwidth limits, and priority queue adjustment to assist packets in achieving the guaranteed rate.

If you have configured prioritization, FortiOS prioritizes egressing packets by distributing them among FIFO (first in, first out) queues associated with each possible priority number. Each physical interface has six priority queues. Virtual interfaces use the priority queues of the physical interface to which they are bound.

Each physical interface's six queues are queue 0 to queue 5, where queue 0 is the highest priority queue. However, you may observe that your traffic uses only a subset of those six queues. For example, some traffic may always use a certain queue number. Queuing may also vary by the packet rate or mixture of services. Some queue numbers may only be used by through traffic for which you have configured traffic shaping in the security policy that applies to that traffic session.

Admin access
Traffic matching security policies with traffic shaping
Traffic matching security policies without traffic shaping
Queue 0
Queue 1
Queue 2
Queue 3
Queue 4
Queue 5
Packets Dropped if:
Rate > Max bandwidth limit
Highest Priority
Lowest Priority

See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822191/traffic-shaping-priority-queueing-priq



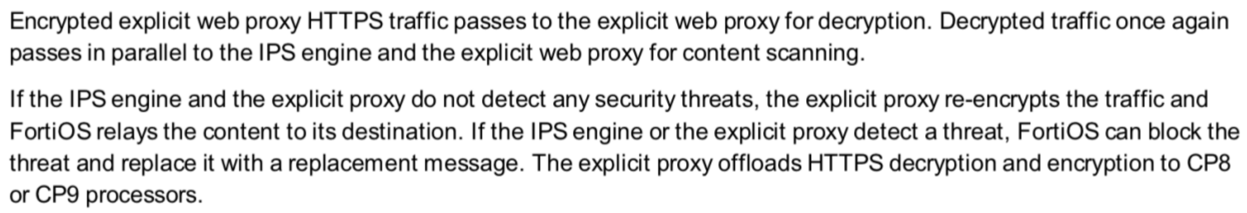
Prioritization and traffic shaping behavior vary based on the configuration, service type, traffic volume, and whether the traffic is through traffic or originates from FortiOS.

Packets can be assigned a priority in one of three ways:

- **On ingress** - for packets flowing through the firewall.
- **Upon generation** - for packets generated by the firewall (including packets generated due to AV proxying).
- **On passing through a firewall policy** - for packets that matches a traffic shaping policy.

See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822191/traffic-shaping-priority-queueing-priq

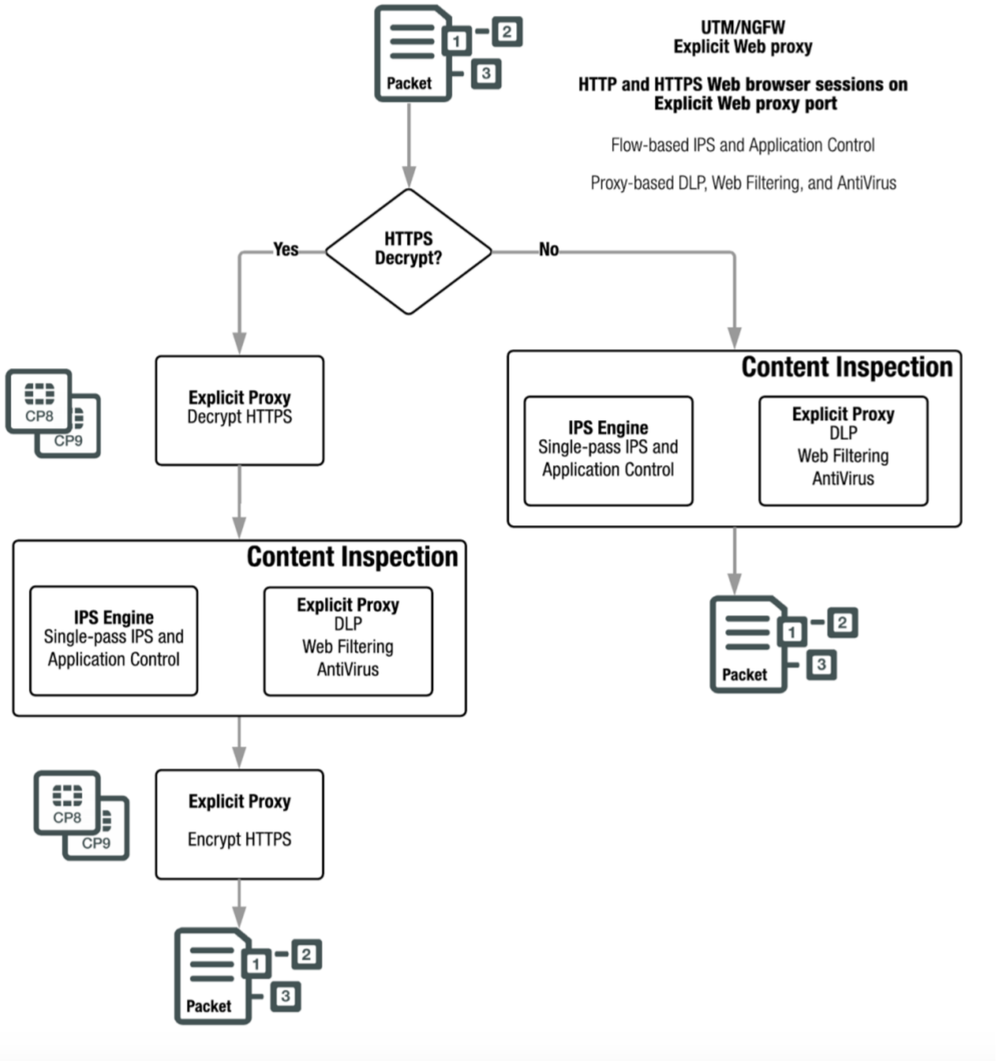
36. On information and belief, the FortiGate-7060E includes a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core.



Encrypted explicit web proxy HTTPS traffic passes to the explicit web proxy for decryption. Decrypted traffic once again passes in parallel to the IPS engine and the explicit web proxy for content scanning.

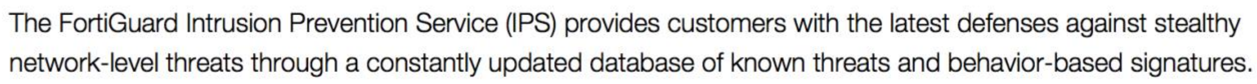
If the IPS engine and the explicit proxy do not detect any security threats, the explicit proxy re-encrypts the traffic and FortiOS relays the content to its destination. If the IPS engine or the explicit proxy detect a threat, FortiOS can block the threat and replace it with a replacement message. The explicit proxy offloads HTTPS decryption and encryption to CP8 or CP9 processors.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 23 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



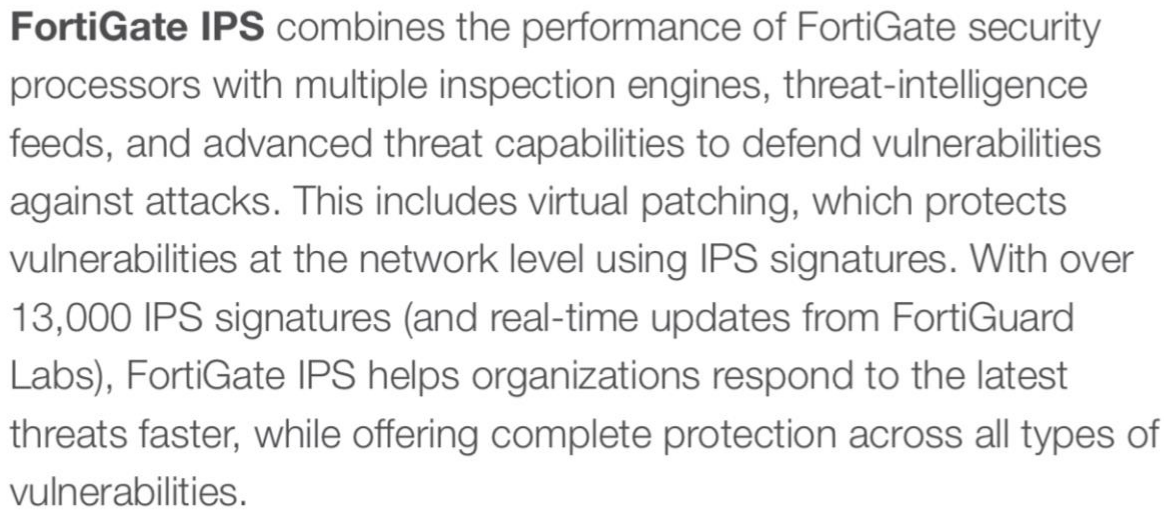
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 22 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

37. On information and belief, the FortiGate-7060E includes a signature database.



The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

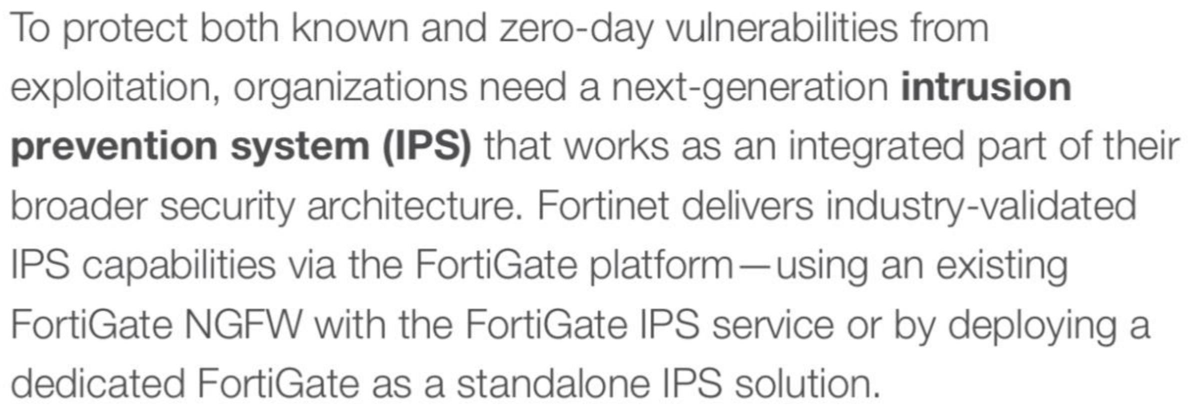
See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips



FortiGate IPS combines the performance of FortiGate security processors with multiple inspection engines, threat-intelligence feeds, and advanced threat capabilities to defend vulnerabilities against attacks. This includes virtual patching, which protects vulnerabilities at the network level using IPS signatures. With over 13,000 IPS signatures (and real-time updates from FortiGuard Labs), FortiGate IPS helps organizations respond to the latest threats faster, while offering complete protection across all types of vulnerabilities.

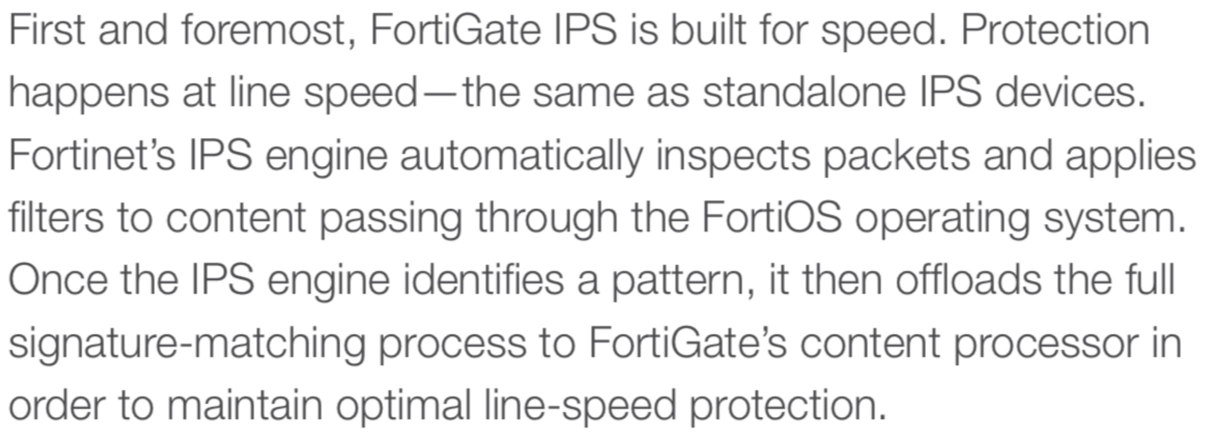
See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf

38. On information and belief, the FortiGate-7060E includes an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.



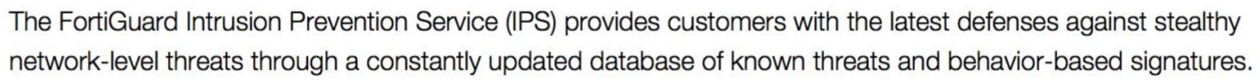
To protect both known and zero-day vulnerabilities from exploitation, organizations need a next-generation **intrusion prevention system (IPS)** that works as an integrated part of their broader security architecture. Fortinet delivers industry-validated IPS capabilities via the FortiGate platform—using an existing FortiGate NGFW with the FortiGate IPS service or by deploying a dedicated FortiGate as a standalone IPS solution.

See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf



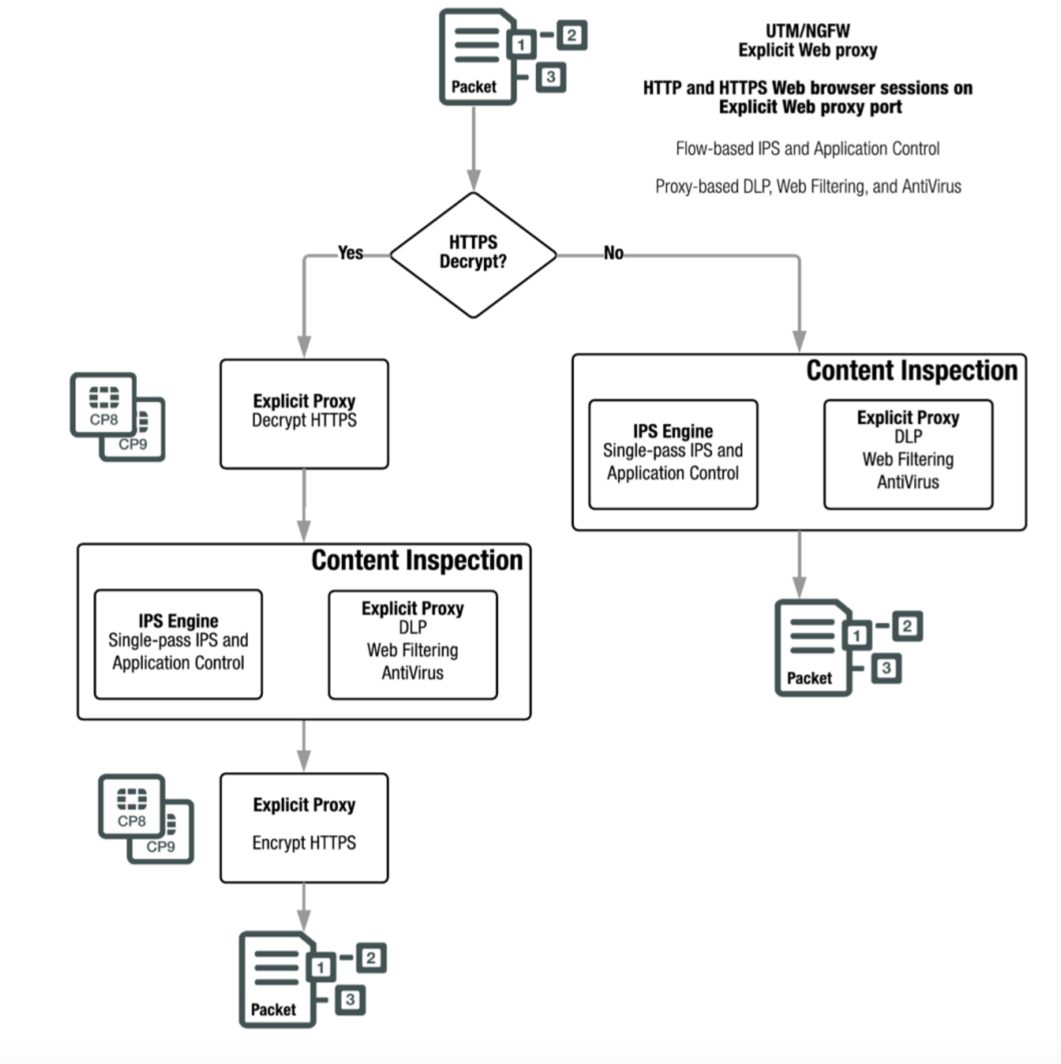
First and foremost, FortiGate IPS is built for speed. Protection happens at line speed—the same as standalone IPS devices. Fortinet's IPS engine automatically inspects packets and applies filters to content passing through the FortiOS operating system. Once the IPS engine identifies a pattern, it then offloads the full signature-matching process to FortiGate's content processor in order to maintain optimal line-speed protection.

See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf



The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips



See FortiOS - Parallel Path Processing (Life of a Packet) at p. 22 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

Count 3 – Claim for infringement of the '323 patent.

39. Lionra incorporates by reference each of the allegations in paragraphs 1–38 above and further alleges as follows:

40. On April 5, 2011, the United States Patent and Trademark Office issued U.S. Patent No. 7,921,323, entitled "Reconfigurable Communications Infrastructure for ASIC Networks." Ex. 3.

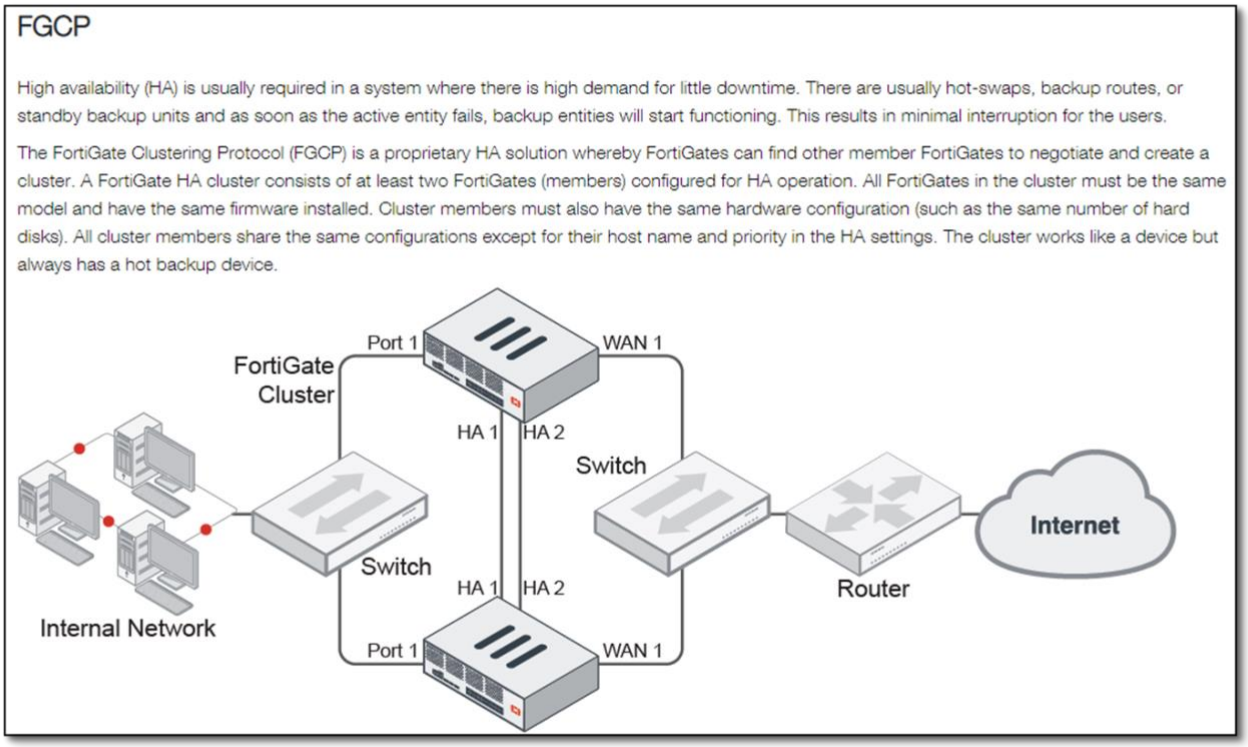
41. Lionra is the owner of the ’323 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

42. Each claim of the ’323 patent is valid, enforceable, and patent-eligible.

43. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’323 patent, and Lionra is entitled to damages for Defendant’s past infringement.

44. Defendant has directly infringed (literally and equivalently) and induced others to infringe the ’323 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’323 patent and by inducing others to infringe the claims of the ’323 patent without a license or permission from Lionra. These products include without limitation the FortiGate 7121F, which infringes at least claim 27 of the ’323 patent.

45. On information and belief, the FortiGate 7121F is designed and intended for use in a communications infrastructure, comprising two or more separate signal processing circuits:



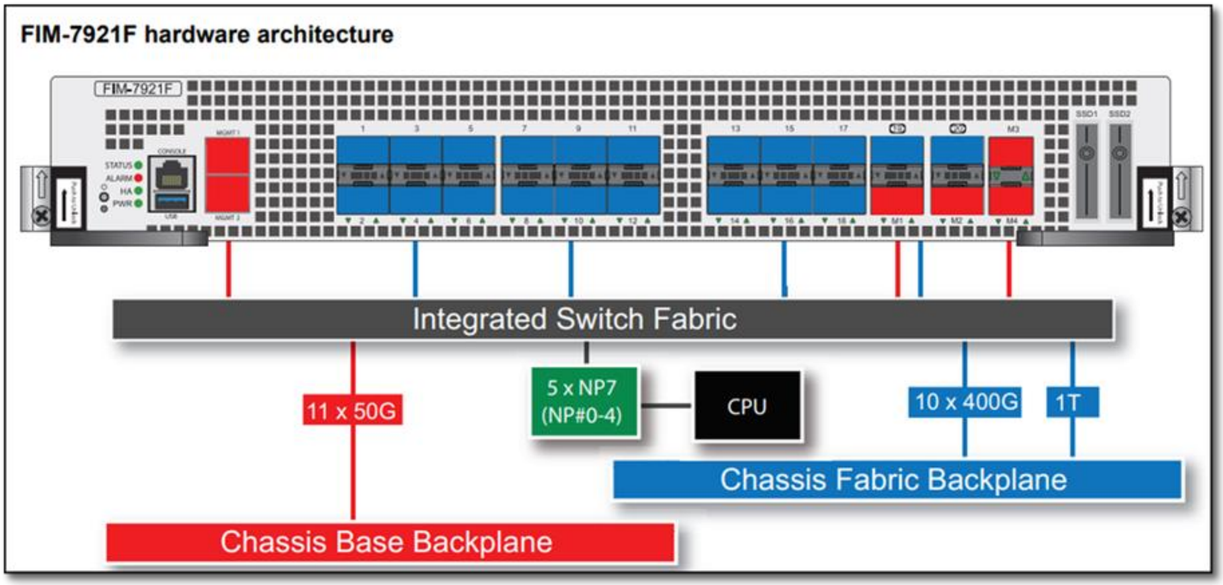
FGCP

High availability (HA) is usually required in a system where there is high demand for little downtime. There are usually hot-swaps, backup routes, or standby backup units and as soon as the active entity fails, backup entities will start functioning. This results in minimal interruption for the users.

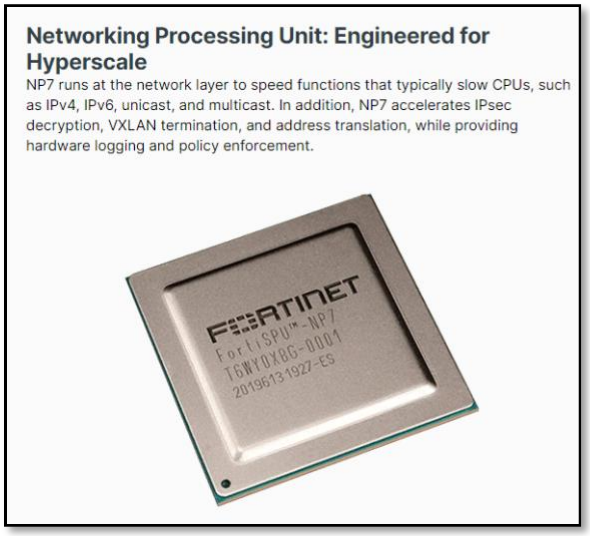
The FortiGate Clustering Protocol (FGCP) is a proprietary HA solution whereby FortiGates can find other member FortiGates to negotiate and create a cluster. A FortiGate HA cluster consists of at least two FortiGates (members) configured for HA operation. All FortiGates in the cluster must be the same model and have the same firmware installed. Cluster members must also have the same hardware configuration (such as the same number of hard disks). All cluster members share the same configurations except for their host name and priority in the HA settings. The cluster works like a device but always has a hot backup device.

See https://docs.fortinet.com/document/fortigate/7.2.1/administration-guide/62403/fgcp

46. On information and belief, each one of said two or more signal processing circuits includes multiple ASIC devices that each itself includes a packet router:



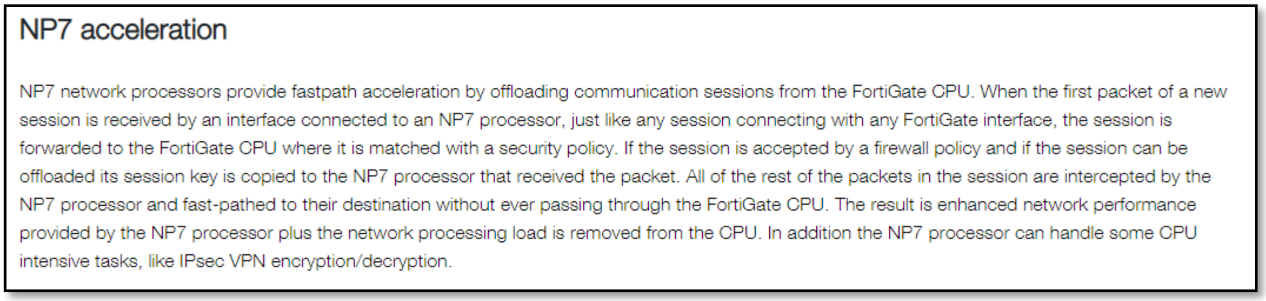
See https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/606554ae-9284-11eb-b70b-00505692583a/fim-7921F-guide.pdf at 12.



Networking Processing Unit: Engineered for Hyperscale

NP7 runs at the network layer to speed functions that typically slow CPUs, such as IPv4, IPv6, unicast, and multicast. In addition, NP7 accelerates IPsec decryption, VXLAN termination, and address translation, while providing hardware logging and policy enforcement.

See https://www.fortinet.com/products/fortigate/fortiasic#np7

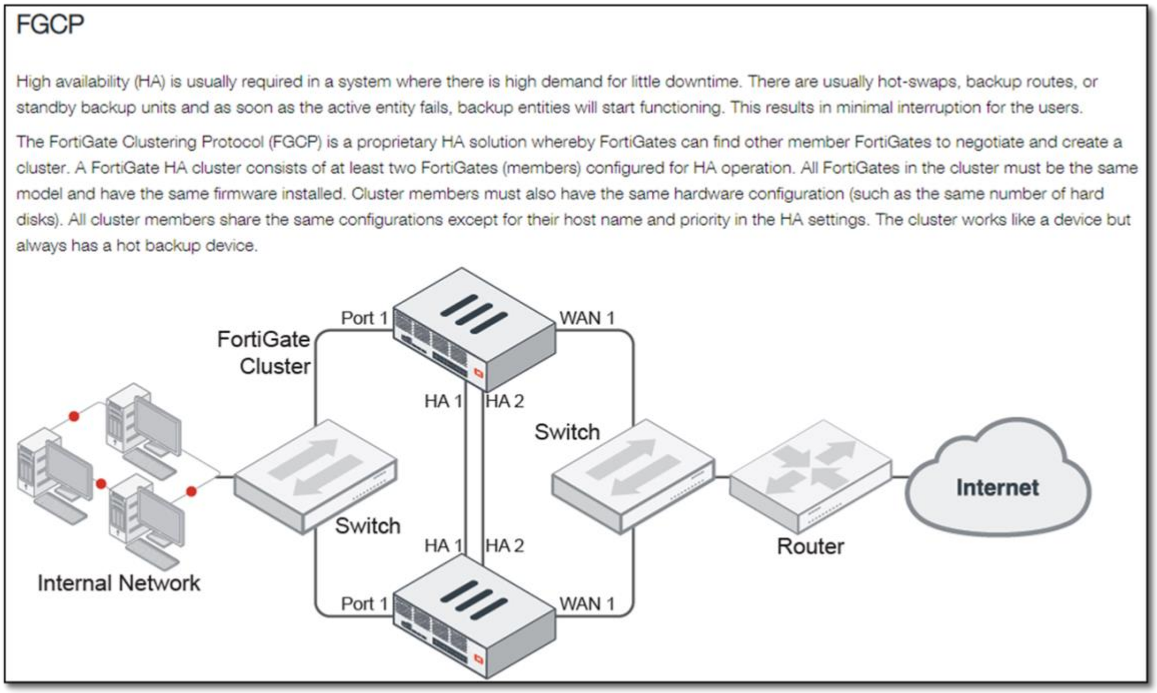


NP7 acceleration

NP7 network processors provide fastpath acceleration by offloading communication sessions from the FortiGate CPU. When the first packet of a new session is received by an interface connected to an NP7 processor, just like any session connecting with any FortiGate interface, the session is forwarded to the FortiGate CPU where it is matched with a security policy. If the session is accepted by a firewall policy and if the session can be offloaded its session key is copied to the NP7 processor that received the packet. All of the rest of the packets in the session are intercepted by the NP7 processor and fast-pathed to their destination without ever passing through the FortiGate CPU. The result is enhanced network performance provided by the NP7 processor plus the network processing load is removed from the CPU. In addition the NP7 processor can handle some CPU intensive tasks, like IPsec VPN encryption/decryption.

See https://docs.fortinet.com/document/fortigate/6.0.0/hardware-acceleration/765824/np7-acceleration

47. On information and belief, said packet router of each one of said ASIC devices of each given one of said respective two or more signal processing circuits being coupled through respective first and second common interfaces and an intervening high speed serial optical link to a respective packet router of each of the ASIC devices of each other of said two or more signal processing circuits with no other processing device intervening between the high speed optical link and said ASIC devices of each of said two or more signal processing circuits:

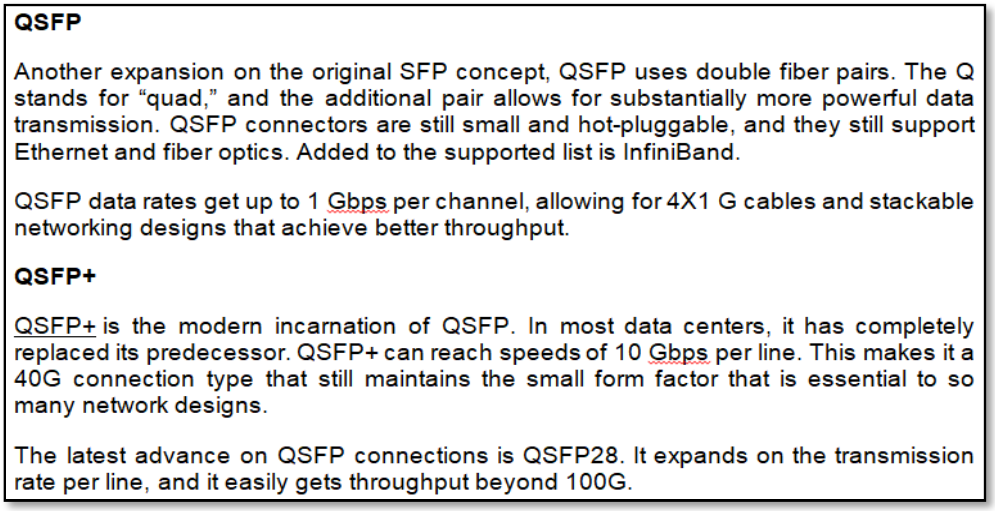


FGCP

High availability (HA) is usually required in a system where there is high demand for little downtime. There are usually hot-swaps, backup routes, or standby backup units and as soon as the active entity fails, backup entities will start functioning. This results in minimal interruption for the users.

The FortiGate Clustering Protocol (FGCP) is a proprietary HA solution whereby FortiGates can find other member FortiGates to negotiate and create a cluster. A FortiGate HA cluster consists of at least two FortiGates (members) configured for HA operation. All FortiGates in the cluster must be the same model and have the same firmware installed. Cluster members must also have the same hardware configuration (such as the same number of hard disks). All cluster members share the same configurations except for their host name and priority in the HA settings. The cluster works like a device but always has a hot backup device.

See https://docs.fortinet.com/document/fortigate/7.2.1/administration-guide/62403/fgcp



QSFP

Another expansion on the original SFP concept, QSFP uses double fiber pairs. The Q stands for “quad,” and the additional pair allows for substantially more powerful data transmission. QSFP connectors are still small and hot-pluggable, and they still support Ethernet and fiber optics. Added to the supported list is InfiniBand.

QSFP data rates get up to 1 Gbps per channel, allowing for 4X1 G cables and stackable networking designs that achieve better throughput.

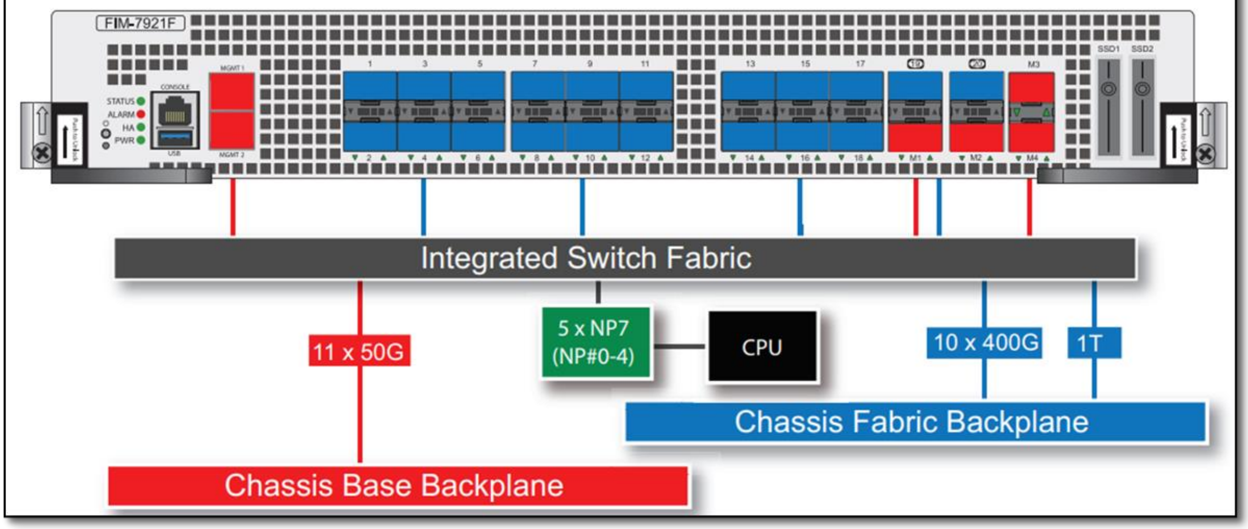
QSFP+

QSFP+ is the modern incarnation of QSFP. In most data centers, it has completely replaced its predecessor. QSFP+ can reach speeds of 10 Gbps per line. This makes it a 40G connection type that still maintains the small form factor that is essential to so many network designs.

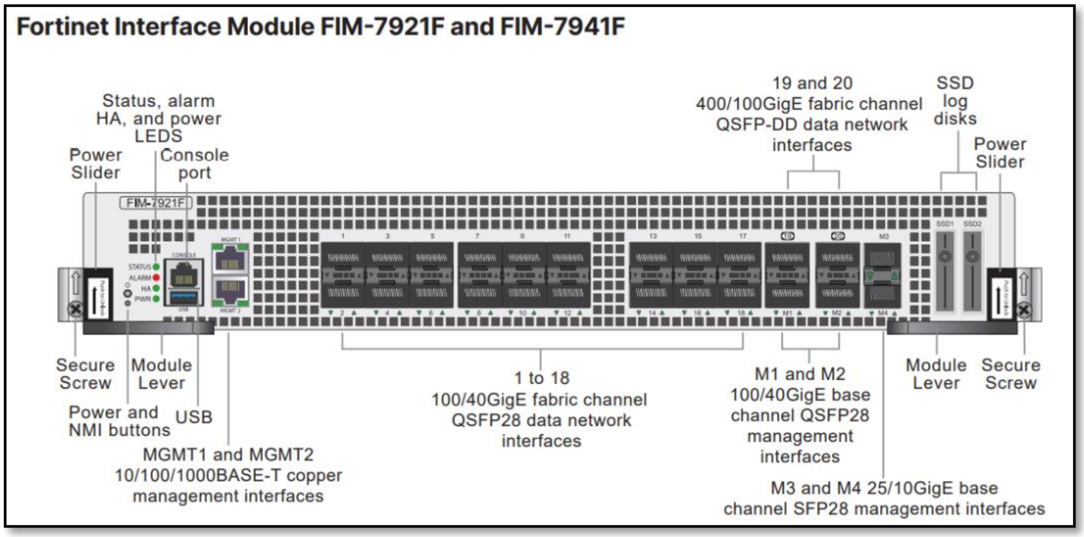
The latest advance on QSFP connections is QSFP28. It expands on the transmission rate per line, and it easily gets throughput beyond 100G.

See https://www.cablesandkits.com/learning-center/differences-between-sfp-qsfp

FIM-7921F hardware architecture



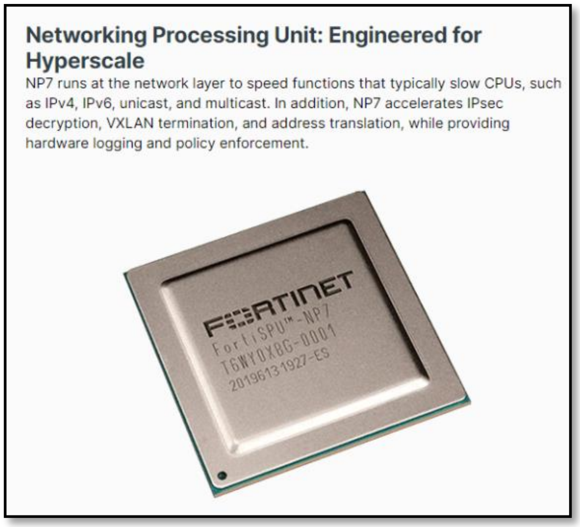
See https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/606554ae-9284-11eb-b70b-00505692583a/fim-7921F-guide.pdf at 12.



Fortinet Interface Module FIM-7921F and FIM-7941F

Status, alarm HA, and power LEDS
Power Slider
Console port
19 and 20 400/100GigE fabric channel QSFP-DD data network interfaces
SSD log disks
Power Slider
FIM-7921F
Secure Screw
Module Lever
Power and NMI buttons
USB
MGMT1 and MGMT2 10/100/1000BASE-T copper management interfaces
1 to 18 100/40GigE fabric channel QSFP28 data network interfaces
M1 and M2 100/40GigE base channel QSFP28 management interfaces
Module Lever
Secure Screw
M3 and M4 25/10GigE base channel SFP28 management interfaces

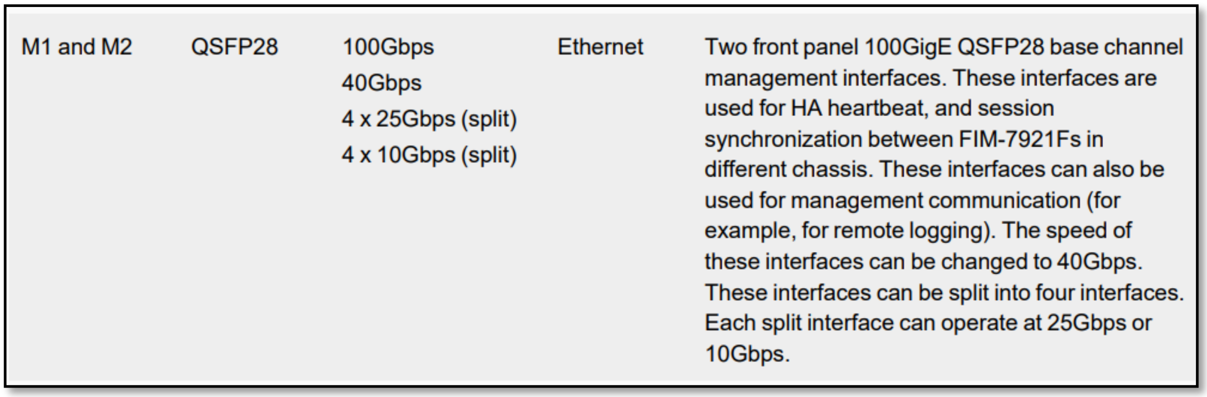
See https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/606554ae-9284-11eb-b70b-00505692583a/fim-7921F-guide.pdf at 5.



Networking Processing Unit: Engineered for Hyperscale

NP7 runs at the network layer to speed functions that typically slow CPUs, such as IPv4, IPv6, unicast, and multicast. In addition, NP7 accelerates IPsec decryption, VXLAN termination, and address translation, while providing hardware logging and policy enforcement.

See https://www.fortinet.com/products/fortigate/fortiasic#np7



M1 and M2	QSFP28	100Gbps 40Gbps 4 x 25Gbps (split) 4 x 10Gbps (split)	Ethernet	Two front panel 100GigE QSFP28 base channel management interfaces. These interfaces are used for HA heartbeat, and session synchronization between FIM-7921Fs in different chassis. These interfaces can also be used for management communication (for example, for remote logging). The speed of these interfaces can be changed to 40Gbps. These interfaces can be split into four interfaces. Each split interface can operate at 25Gbps or 10Gbps.

See https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/606554ae-9284-11eb-b70b-00505692583a/fim-7921F-guide.pdf at 7.

Count 4 – Claim for infringement of the ’612 patent.

48. Lionra incorporates by reference each of the allegations in paragraphs 1–47 above and further alleges as follows:

49. On October 22, 2013, the United States Patent and Trademark Office issued U.S. Patent No. 7,856,612, entitled “System and Method for a Secure I/O Interface.” Ex. 4.

50. Lionra is the owner of the ’612 patent with full rights to pursue recovery of royalties for damages for infringement, including full rights to recover past and future damages.

51. Each claim of the ’612 patent is valid, enforceable, and patent-eligible.

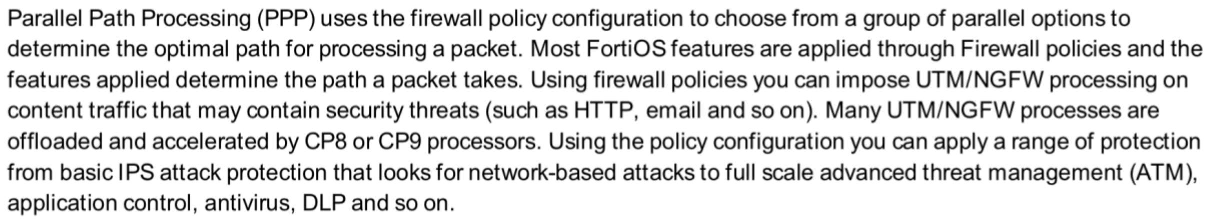
52. Lionra and its predecessors in interest have satisfied the requirements of 35 U.S.C. § 287(a) with respect to the ’612 patent, and Lionra is entitled to damages for Defendant’s past infringement.

53. Defendant have directly infringed (literally and equivalently) and induced others to infringe the ’612 patent by making, using, selling, offering for sale, or importing products that infringe the claims of the ’612 patent and by inducing others to infringe the claims of the ’612 patent without

a license or permission from Lionra. These products include without limitation Defendant's FortiGate-7060E, which infringes at least claim 1 of the '612 patent.

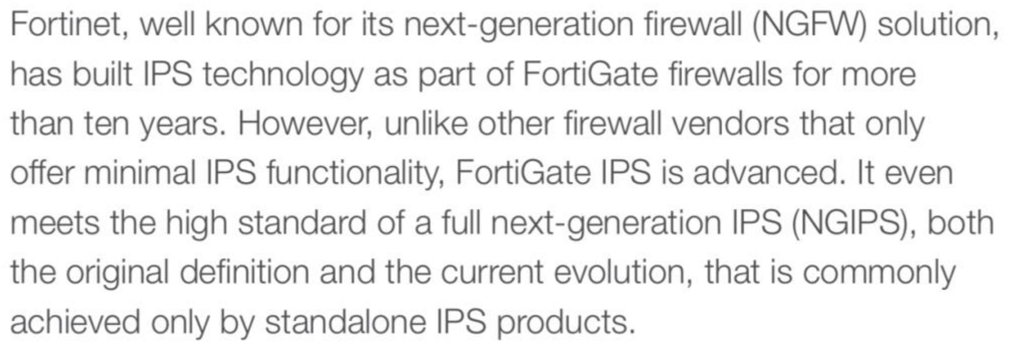
54. Defendant also has indirectly infringed at least one claim of the '612 patent contributorily under 35 U.S.C. § 271(c) by offering to sell and selling the Accused Products, knowing the same to be especially made or especially adapted for use in an infringement of the '612 patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use. They do not have any substantial non-infringing uses.

55. On information and belief, whether or not the preamble is limiting, FortiGate-7060E is a security processor for processing incoming packets and outgoing packets.



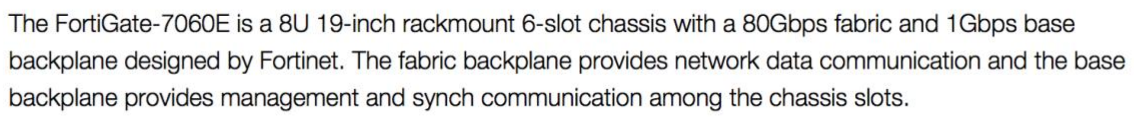
Parallel Path Processing (PPP) uses the firewall policy configuration to choose from a group of parallel options to determine the optimal path for processing a packet. Most FortiOS features are applied through Firewall policies and the features applied determine the path a packet takes. Using firewall policies you can impose UTM/NGFW processing on content traffic that may contain security threats (such as HTTP, email and so on). Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors. Using the policy configuration you can apply a range of protection from basic IPS attack protection that looks for network-based attacks to full scale advanced threat management (ATM), application control, antivirus, DLP and so on.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 6 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



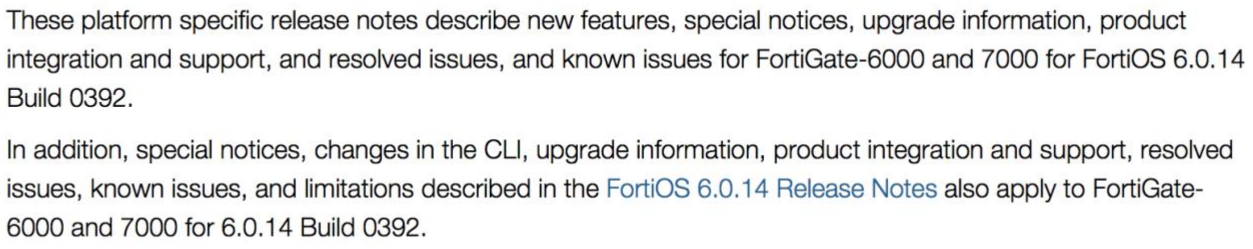
Fortinet, well known for its next-generation firewall (NGFW) solution, has built IPS technology as part of FortiGate firewalls for more than ten years. However, unlike other firewall vendors that only offer minimal IPS functionality, FortiGate IPS is advanced. It even meets the high standard of a full next-generation IPS (NGIPS), both the original definition and the current evolution, that is commonly achieved only by standalone IPS products.

See Powerful and Innovative Intrusion Prevention Systems FortiGate IPS at p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-FortiGateIPS.pdf



The FortiGate-7060E is a 8U 19-inch rackmount 6-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

See https://docs.fortinet.com/document/fortigate/6.0.14/fortigate-7000-documents/64586/fortigate-7060e

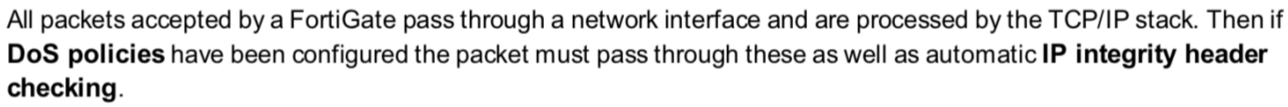


These platform specific release notes describe new features, special notices, upgrade information, product integration and support, and resolved issues, and known issues for FortiGate-6000 and 7000 for FortiOS 6.0.14 Build 0392.

In addition, special notices, changes in the CLI, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.0.14 Release Notes also apply to FortiGate-6000 and 7000 for 6.0.14 Build 0392.

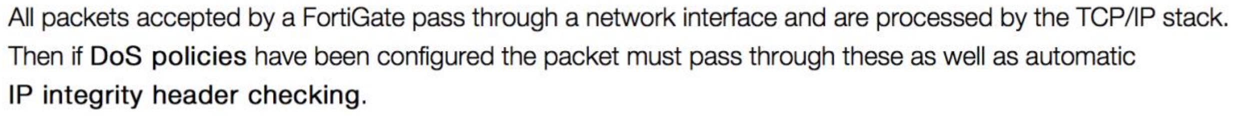
See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000-release-notes/575159/fortigate-6000-and-fortigate-7000-6-0-14-release-notes

56. On information and belief, the *FortiGate*-7060E includes a switching system to send the outgoing packets and receive the incoming packets.



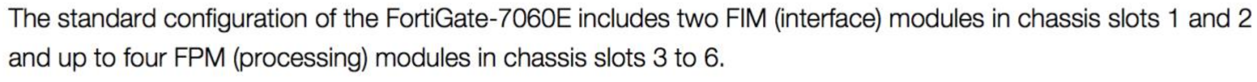
All packets accepted by a FortiGate pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking**.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 9 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



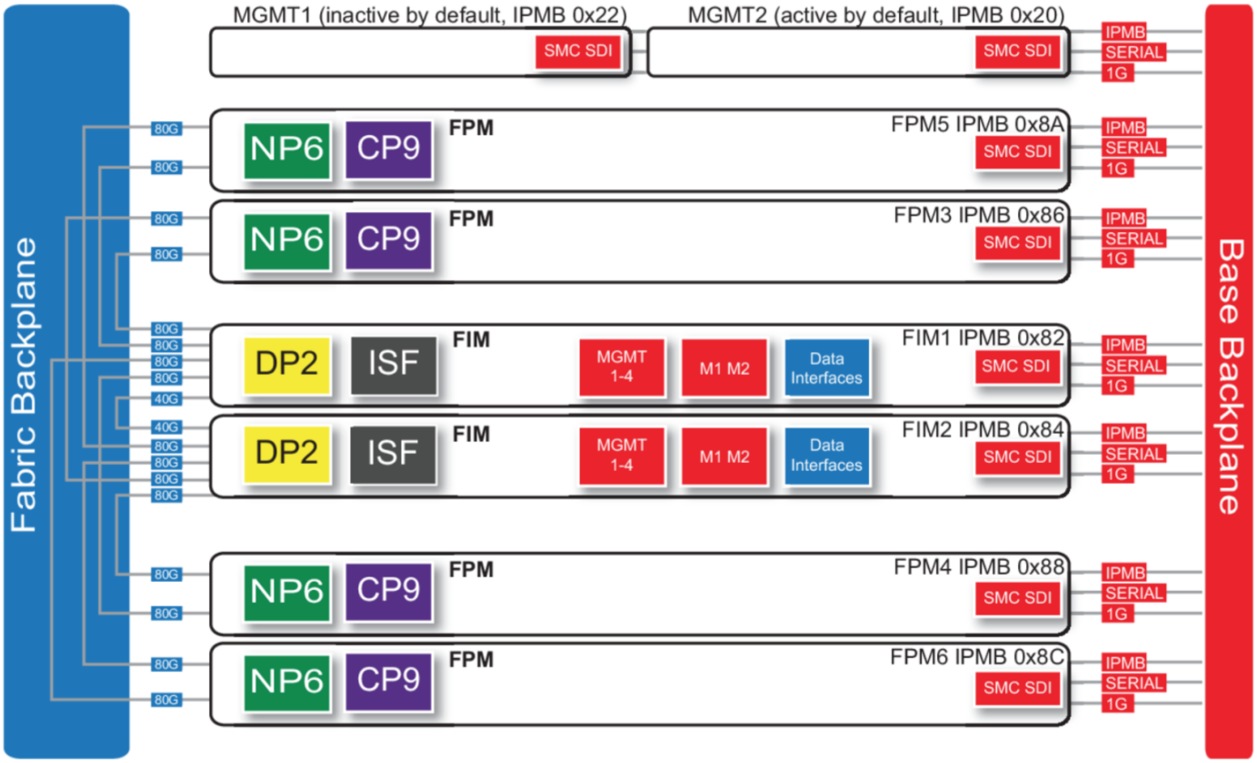
All packets accepted by a FortiGate pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking.**

See https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

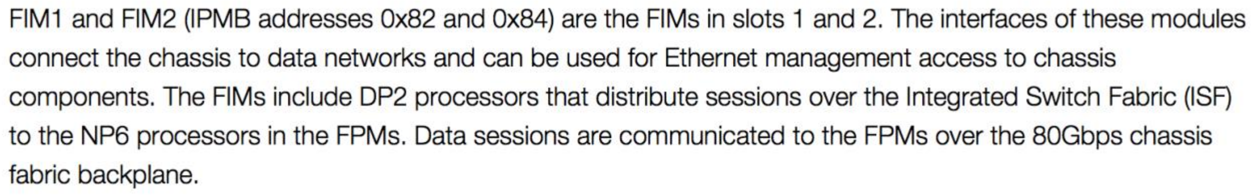


The standard configuration of the FortiGate-7060E includes two FIM (interface) modules in chassis slots 1 and 2 and up to four FPM (processing) modules in chassis slots 3 to 6.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e



See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e

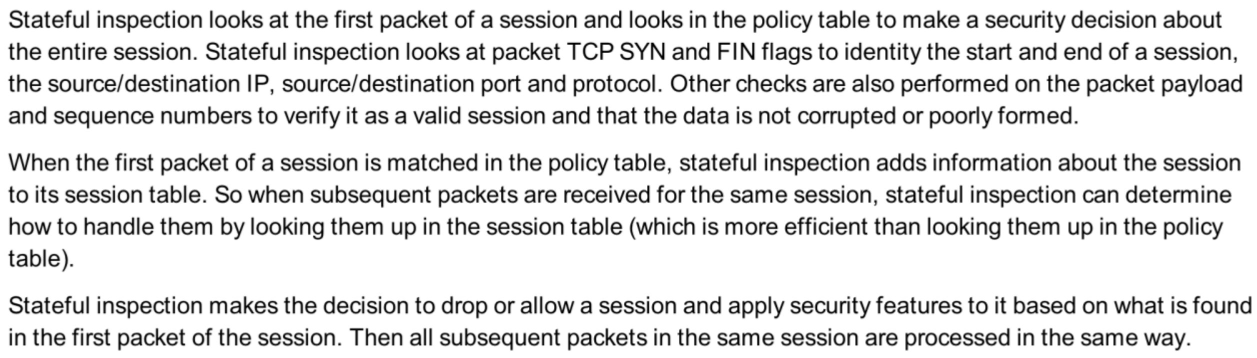


FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

See https://docs.fortinet.com/document/fortigate-7000/6.0.14/fortigate-7000E-handbook/64586/fortigate-7060e

57. On information and belief, the FortiGate-7060E includes a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the

switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

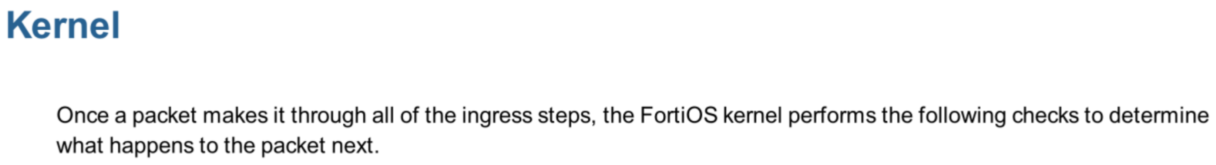


Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed.

When the first packet of a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).

Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way.

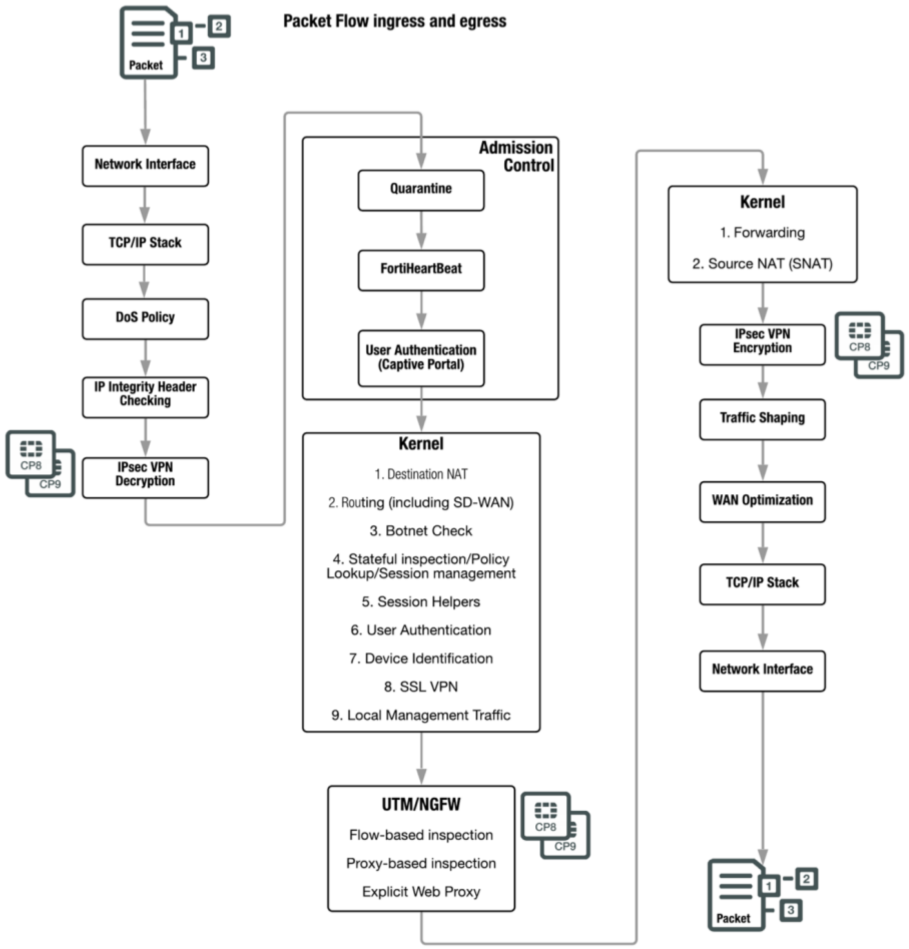
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 10 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



Kernel

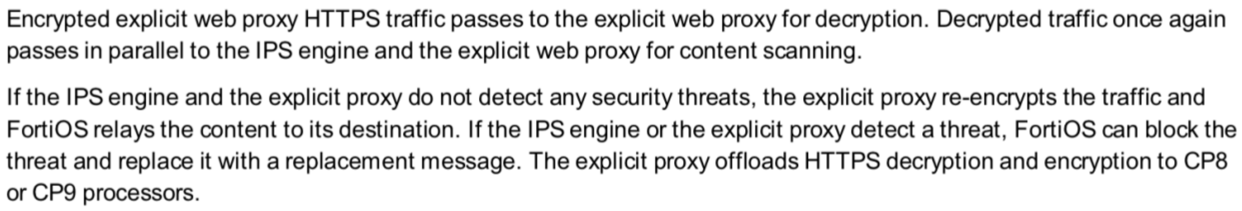
Once a packet makes it through all of the ingress steps, the FortiOS kernel performs the following checks to determine what happens to the packet next.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 9 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



See FortiOS - Parallel Path Processing (Life of a Packet) at p. 8 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

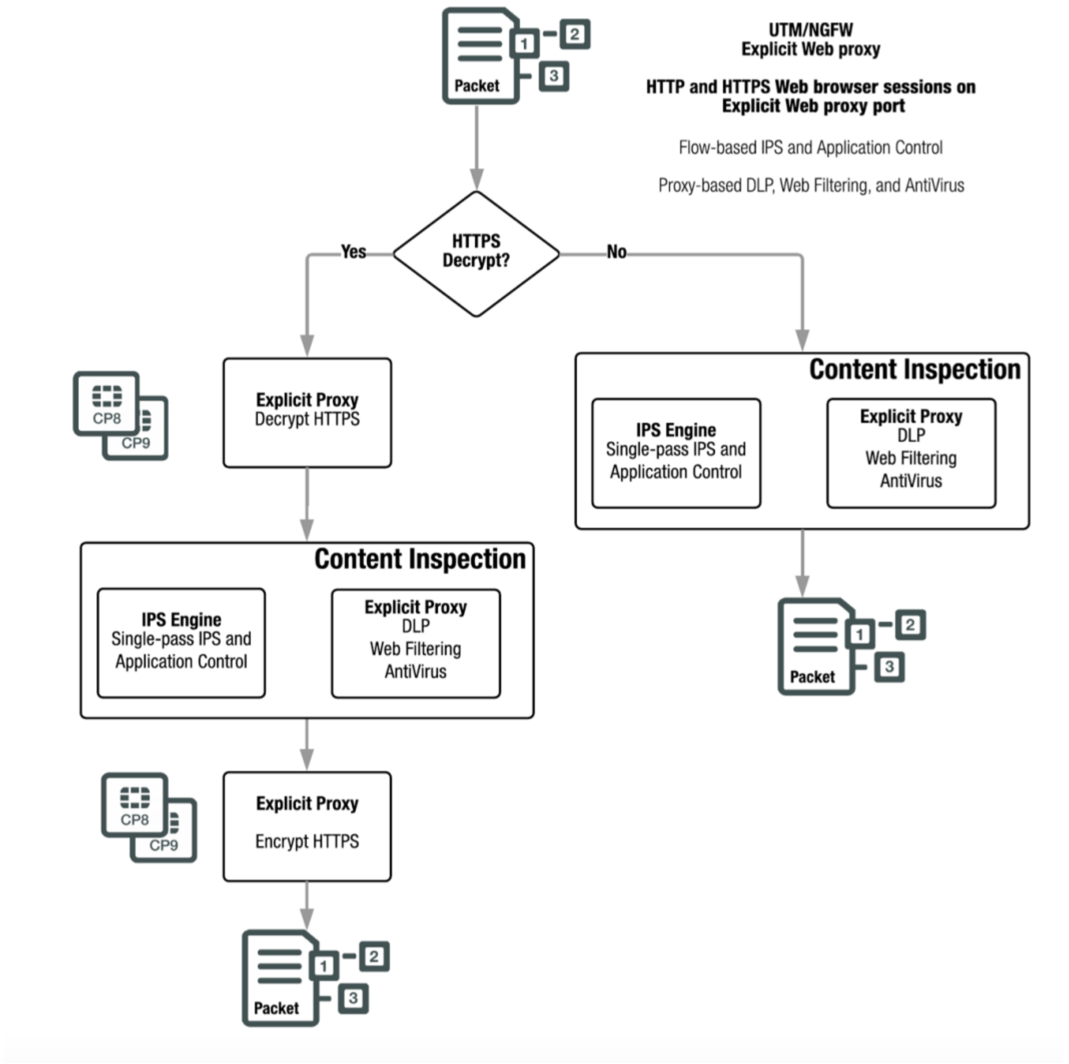
58. On information and belief, the FortiGate-7060E includes a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core.



Encrypted explicit web proxy HTTPS traffic passes to the explicit web proxy for decryption. Decrypted traffic once again passes in parallel to the IPS engine and the explicit web proxy for content scanning.

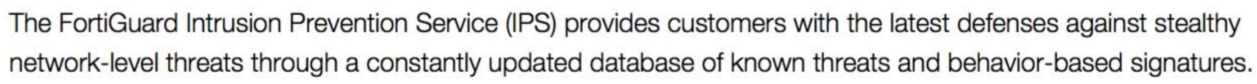
If the IPS engine and the explicit proxy do not detect any security threats, the explicit proxy re-encrypts the traffic and FortiOS relays the content to its destination. If the IPS engine or the explicit proxy detect a threat, FortiOS can block the threat and replace it with a replacement message. The explicit proxy offloads HTTPS decryption and encryption to CP8 or CP9 processors.

See FortiOS - Parallel Path Processing (Life of a Packet) at p. 23 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading



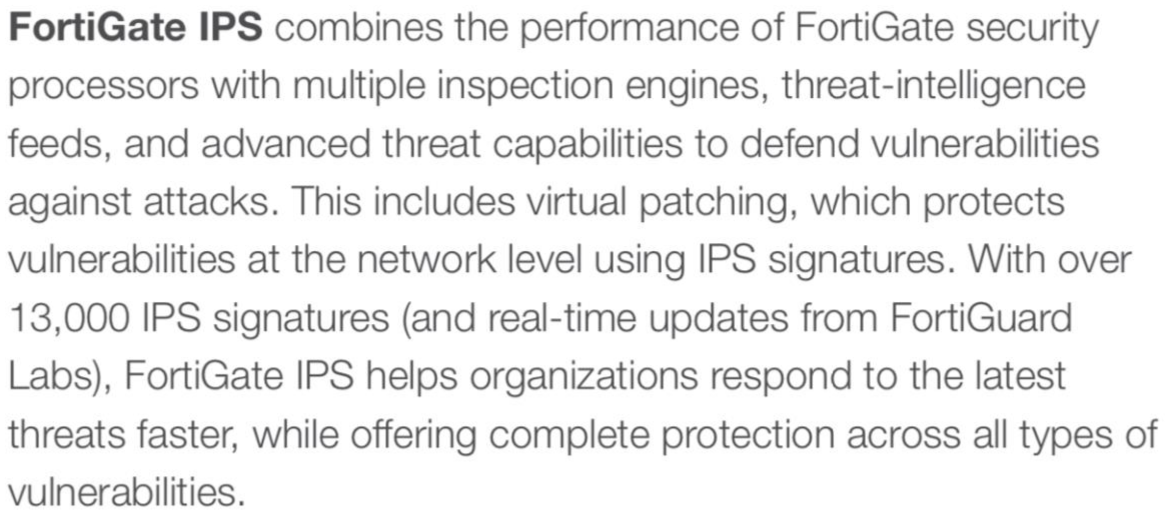
See FortiOS - Parallel Path Processing (Life of a Packet) at p. 22 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

59. On information and belief, the FortiGate-7060E includes a signature database.



The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

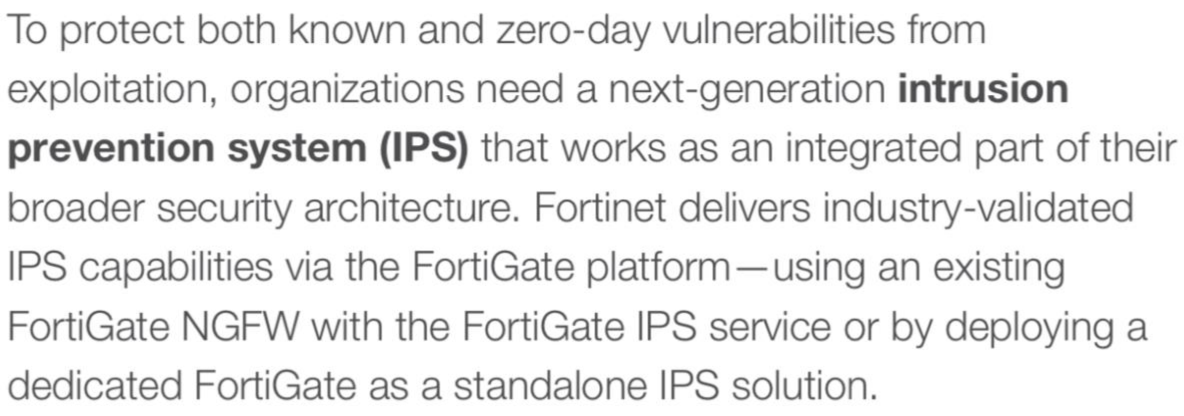
See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips



FortiGate IPS combines the performance of FortiGate security processors with multiple inspection engines, threat-intelligence feeds, and advanced threat capabilities to defend vulnerabilities against attacks. This includes virtual patching, which protects vulnerabilities at the network level using IPS signatures. With over 13,000 IPS signatures (and real-time updates from FortiGuard Labs), FortiGate IPS helps organizations respond to the latest threats faster, while offering complete protection across all types of vulnerabilities.

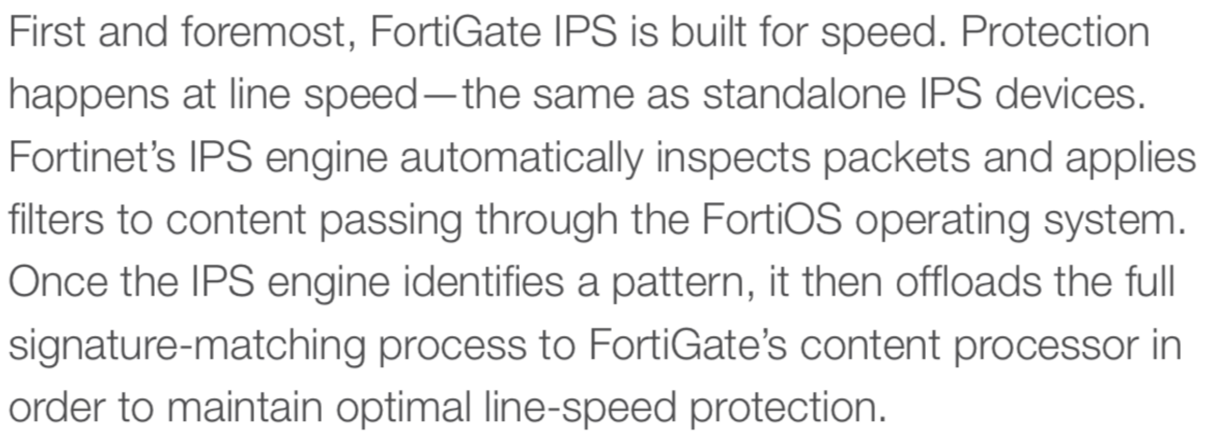
See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf

60. On information and belief, the FortiGate-7060E includes an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.



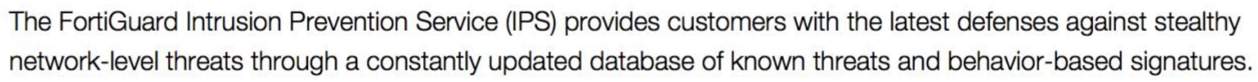
To protect both known and zero-day vulnerabilities from exploitation, organizations need a next-generation **intrusion prevention system (IPS)** that works as an integrated part of their broader security architecture. Fortinet delivers industry-validated IPS capabilities via the FortiGate platform—using an existing FortiGate NGFW with the FortiGate IPS service or by deploying a dedicated FortiGate as a standalone IPS solution.

See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf



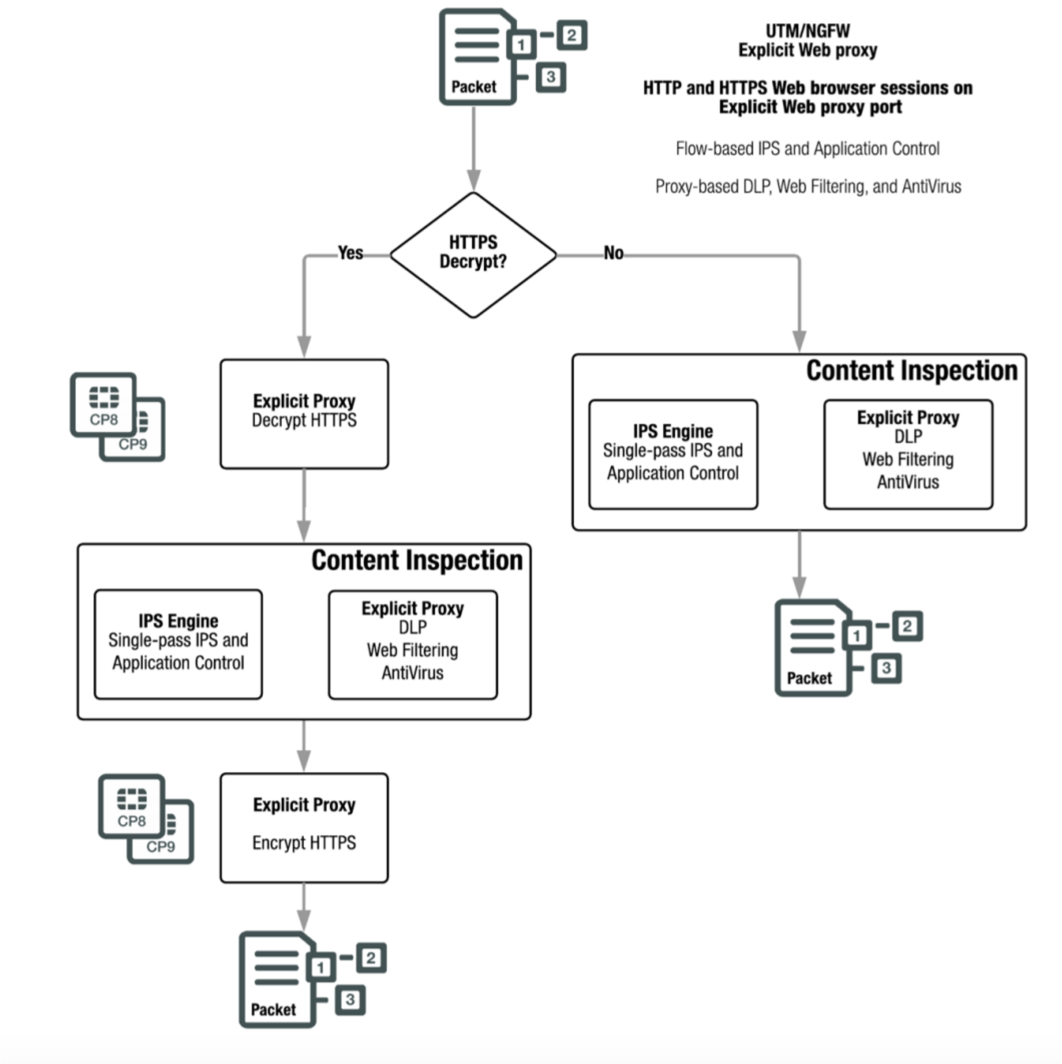
First and foremost, FortiGate IPS is built for speed. Protection happens at line speed—the same as standalone IPS devices. Fortinet's IPS engine automatically inspects packets and applies filters to content passing through the FortiOS operating system. Once the IPS engine identifies a pattern, it then offloads the full signature-matching process to FortiGate's content processor in order to maintain optimal line-speed protection.

See Mitigating Vulnerabilities: A FortiGate IPS Overview p. 2 available at https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf



The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

See https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips



See FortiOS - Parallel Path Processing (Life of a Packet) at p. 22 available at https://docs.fortinet.com/document/fortigate/6.0.0/parallel-path-processing-life-of-a-packet/478386/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

Jury Trial Demanded

61. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Lionra requests a trial by jury of any issues so triable by right.

Prayer for Relief

Plaintiff Lionra respectfully requests the following relief from this Court:

A. A judgment in favor of Lionra that Defendant have infringed the ’708, ’436, ’323, and ’612 patents, and that the ’708, ’436, ’323, and ’612 patents are valid, enforceable, and patent-eligible;

B. A judgment and order requiring Defendant to pay Lionra compensatory damages, costs, expenses, and pre- and post-judgment interest for its infringement of the asserted patents, as provided under 35 U.S.C. § 284;

C. Any and all injunctive and/or equitable relief to which Lionra may be entitled including, but not limited to, ongoing royalties with respect to Defendant’s infringement of the ’708, ’436, ’323, and ’612 patents;

D. A judgment and order requiring Defendant to provide an accounting and to pay supplemental damages to Lionra, including, without limitation, pre-judgment and post-judgment interest;

E. A finding that this case is exceptional under 35 U.S.C. § 285, and an award of Lionra’s reasonable attorney’s fees and costs; and

F. Any and all other relief to which Lionra may be entitled.

Dated: August 19, 2022

/s/ Reza Mirzaie

Reza Mirzaie
CA State Bar No. 246953
Marc A. Fenster
CA State Bar No. 181067
Paul A. Kroeger
CA State Bar No. 229074
Neil A. Rubin
CA State Bar No. 250761
Jonathan Ma
CA State Bar No. 312773
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
Telephone: 310-826-7474
Email: rmirzaie@raklaw.com
Email: mfenster@raklaw.com
Email: pkroeger@raklaw.com
Email: nrubin@raklaw.com
Email: jma@raklaw.com

ATTORNEYS FOR PLAINTIFF,
LIONRA TECHNOLOGIES LIMITED